New Proxy Blind Signcryption Scheme for Secure Multiple Digital Messages Transmission Based on Elliptic Curve Cryptography

Pin-Chang Su[1] and Chien-Hua Tsai[2*]
[1] Department of Information Management, National Defense University
4F #7, Aly. 10, Ln. 35, Bau-Yi Street, Sijhih District, New Taipei City 221 - TAIWAN
[e-mail: spc.cg@msa.hinet.net]
[2] Department of Accounting Information, Chihlee University of Technology
7F-5, #136, Cheng-Yi North Road, Sanchung District, New Taipei City 241 - TAIWAN
[e-mail: chienhua@mail.chihlee.edu.tw]
*Corresponding author: Chien-Hua Tsai

Received March 10, 2017; revised June 11, 2017; accepted July 10, 2017; published November 30, 2017

Abstract

Having the characteristics of unlinkability, anonymity, and unforgeability, blind signatures are widely used for privacy-related applications such as electronic cash, electronic voting and electronic auction systems where to maintain the anonymity of the participants. Among these applications, the blinded message is needed for a certain purpose by which users delegate signing operation and communicate with each other in a trusted manner. This application leads to the need of proxy blind signature schemes. Proxy blind signature is an important type of cryptographic primitive to realize the properties of both blind signature and proxy signature. Over the past years, many proxy blind signature algorithms have been adopted to fulfill such task based on the discrete logarithm problem (DLP) and the elliptic curve discrete log problem (ECDLP), and most of the existing studies mainly aim to provide effective models to satisfy the security requirements concerning a single blinded message. Unlike many previous works, the proposed scheme applies the signcryption paradigm to the proxy blind signature technology for handling multiple blinded messages at a time based on elliptic curve cryptography (ECC). This innovative method thus has a higher level of security to achieve the security goals of both blind signature and proxy signature. Moreover, the evaluation results show that this proposed protocol is more efficient, consuming low communication overhead while increasing the volume of digital messages compared to the performance from other solutions. Due to these features, this design is able to be implemented in small low-power intelligent devices and very suitable and easily adoptable for e-system applications in pervasive mobile computing environment.

Keywords: Proxy blind signature, Signcryption, Elliptic curve cryptography

1. Introduction

With the widespread utilization of computers, mobile devices and computing applications, information technology has made it possible to gather people's information in historically unparalleled ways. In order to prevent individuals' privacy from the corresponding identifiers on the Internet, various security practices have been adopted to keep private information confidential. The technology of blind signatures, for example, has been proposed to anonymously protect identifiable individuals from being revealed to other individuals or groups. In 1983, Chaum [1] first described the concept of blind signature in which the content of messages has to remain concelaed from the signer who cannot link the message-signature pair to its signing session [2][3] even if the signature is exposed by other users later. Because of the unforgeability and unlinkability (or blindness) properties of [4][5], blind signature schemes are extensively employed in many variants of privacy-related applications to such issues as e-voting, e-cash and e-auction systems [6][7] and [8].

In these e-system applications particularly for distributed shared object systems, mobile network communications and grid computing environments [9][10] and [11], there is a need for a proxy signature protocol which allows an entity, called the original signer, to delegate the privileges of signing to another entity, called the proxy signer. The proxy signer can create a proxy signature and any verifier can validate its correctness by the given verification procedure. The notation of a proxy signature scheme was first introduced by Mambo et al. [12] in 1996, and several essential considerations have been shown to increase the security properties of a proxy signature scheme in terms of non-repudiation, unforgeability, verification, etc. A number of proxy signature methodologies have been proposed to address various security requirements [13][14][15][16][17] and [18], since then. Soon afterwards, having combined both the proxy signature and blind signature, Lin and Jan [19] were the first that explained the idea of a proxy blind signature unique structure in 2000. With such attributes, the proxy signer is delegated to generate a blind signature which is similar to a digital signature but not quite the same, on behalf of the original signer.

Followed by the first construction given, Tan et al. [20] then introduce a new proxy blind signature schemes based on DLP (the discrete logarithm problem) and ECDLP (the elliptic curve discrete log problem), which enhances the security measures of proxy blind signature schemes. Awasthi and Lal [21] subsequently propose a more efficient and secure proxy blind signature scheme and point out that Tan et al.'s scheme suffers from a type of forgery attack due to the signature receiver. Sun et al. [22] simultaneously show that Tan et al.'s scheme doesn't satisfy the unforgeability and unlinkability properties. In addition, they also specify that Awasthi and Lal's scheme does not possess the unlinkability property either. After that Wang and Wang [23] contribute a proxy blind signature scheme based on ECDLP. However, Yang and Yu [24] prove that Wang and Wang's scheme fails to provide the security properties like unforgeability, non-repudiation and unlinkability. Moreover, Kar et al. [25] indicate that Yang and Yu's scheme does not conform to the characteristic of unforgeability, and propose an improved secure proxy blind signature scheme based on DLP. Afterwards, the two new proxy blind signatures based on ECDLP have been presented in Pradhan and Mohapatra [26], and Alghazzawi et al. [27] rspectively, and their schemes are still insecure against attacks on the linkability protection methods. Wang and Liao [28] later show that their schemes don't meet the unlinkability property, and also introduce an enhanced construction on ECDLP-based proxy blind signature scheme. The latest ECDLP-based scheme dealing with

proxy blind signatures is Sadat et al. [29], and their work uses the combined functionalities of digital signatures and encryption techniques in a way, called the signcryption scheme, which was first proposed by Zheng [30] in 1997 as a cryptographic primitive, to perform an efficient proxy blind signcryption cryptosystem. Under the concept of signcryption assumption, more efficient proxy and blind signcryption schemes appeared in the literature later on [31][32][33] and [34].

While the above-mentioned studies provide valuable cryptographic models regarding the proxy blind signature, caution needs to be exercised before applying these practices in a real-world setting. Most of these existing ECDLP-based proxy blind signature protocols have an "efficient method," that is, that handles proxy blind signatures in a single message at a time or a batch of multiple signatures on multiple messages [35][36] instead of managing a large number of digital messages by making only one single signature [37], are inefficient. In addition to an efficient implementation of the proxy blind signature procedure, the other concern is that all participants interact with one another in establishing communication sessions of which data can leave an identifier stolen more vulnerable to identity theft or fraud attacks. Despite the fact that the current proxy blind signature solutions are conducted under strict authentication procedures and settings, this vulnerability condition of data leak between sessions can increase the probability of information disclosure.

Unlike the previous approaches that focus proxy blind signatures on one signature at a time or a batch mode, our proposal conducts multiple digital messages by making one time signature to implement a truly efficient protocol. Additionally, the proposed scheme maintains all message blocks to produce the avalanche effect as more and more blocks connect to the subsequent segment, and this security measure is able to prevent information leakage from occurring in each time period. It is worthwhile pointing out that a newly unveiled multiple-document cryptosystem from Tsai and Su's recent works [38][39] in 2015 and 2017, respectively. Of these two signcryption techniques, the former presents a different type of a threshold signcryption protocol by assigning a group of signatures to share a secret link for multiple documents and their study handles a large number of digital documents via a group of participants splitting a secret and each of member is allocated a share of the secret, but the latter introduces an alternative paradigm for a blind signcryption model (viz. a non-designated proxy method) and manages multiple documents by one single person employing a blind signcryption technique along with these messages to enable effective protection measures like the anonymity and untraceability properties. Naturally, it takes the proxy blind signcryption operation from a non-designated proxy perspective into consideration. In some real situations, we must apply this practice, for example, particularly in an anonymous proxy blind e-payment system in a global distributed processing model. This paper is aimed at proposing an efficient proxy blind signcryption scheme that provably satisfy the security properties of both proxy and blind signatures, based on the hardness assumptions of the ECDLP and the permutation shifting problem.

The main contribution of our work not only significantly strengthens the principles of provable security which we give the results of security analysis in Section 4, as pointed out by [21][22][24][26][27] and [28], including unforgeability, non-repudiation and unlinkability, but also innovatively offers a model for proxy-signature-related or blind-signature-related topics on processing multiple digital messages, as exemplified by [37][38] and [39]; likewise we provide a high-performance solution through a vast amount of digital messages in terms of computational efficiency in Section 5. Another contribution of this study is to show that a direct implementation of this scheme describes a process where ciphertext from one block encryption step gets intermixed with the shifted data point from the next encryption step until

the complete sequence of encoded messages is synthesized as an avalanche effect which we present in Section 3. Therefore, with these characteristics, the proposed scheme is extremely suitable for efficient and secure data transmission in mobile computing environments. The paper is organized as follows. In the next section, we briefly introduce the basics of elliptic curve cryptography (ECC), and proxy blind signature protocols based on the elliptic curve discrete log problem (ECDLP). Section 3 presents an original essay to establish a proxy blind signcryption scheme based on ECC for multiple electronic messages. In section 4 and 5, we analyze the security features of the proposed solution and evaluate its efficiency and performance, respectively. Finally, section 6 describes concluding the paper.

2. Preliminary Background and Related Work

Following is the description of background study and related works in the field. A brief overview of the nature of ECC will first be given. Subsequently, we sketch some previous works of the same type with corresponding a proxy blind signature technique based on ECDLP from their respective backgrounds, which will be compared to our proposed scheme in Section 4 and 5.

2.1 Basis of Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) was independently suggested by mathematicians Miller [40] and Koblitz [41] as an alternative for implementing public key cryptosystems in the middle of the 1980s using small key sizes and computational speed to achieve security strength and efficient improvements [42][43]. Normally, an elliptic curve has the form, $y^2 + axy + by = x^3 + cx^2 + dx + e$, where a, b, c, d and e are real numbers. There are some elementary operations in ECC. For example, the point addition operation is defined over elliptic curves, and this with the inclusion of a point ∞, called point at infinity. If three points are on a line that intersects an elliptic curve, then their sum is equal to the point at infinity ∞. If the characteristic of q is neither two nor three (e.g., $K = F_q$ where $q > 3$ is a prime), then an elliptic group over the Galois Field $E(F_q)$ can be obtained by computing $y^2 = x^3 + ax + b \bmod q$ for $0 \le x < q$. The contents a, b are non-negative integers that are smaller than the prime number q and satisfy the condition $4a^3 + 27b^2 \bmod q \neq 0$. Let the points $A=(x_1, y_1)$ and $B=(x_2, y_2)$ be in the elliptic group $E(F_q)$. The rules for addition over the elliptic group $E(F_q)$ are:

- $P + \infty = \infty + P = P$.
- If $x_2 = x_1$ and $y_2 = -y_1$, that is $P = (x_1, y_1)$ and $Q = (x_2, y_2) = (x_1, -y_1) = -P$, then $P + Q = \infty$.
- If $Q \neq P$, then the sum $P + Q = (x_3, y_3)$ is given by

  $x_3 \equiv \lambda^2 - x_1 - x_2 \bmod q$,

  $y_3 \equiv \lambda(x_1 - x_3) - y_1 \bmod q$,

  where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ if $x_1 \neq x_2$ or $\lambda = (3x_1^2 + a)/2y_1$ if $x_1 = x_2$ and y_1.

To double for a point P, it is equivalent to do $P + P$. Similarly, we can calculate $3P = 2P + P$ and so on. As just mentioned, ECC is based on the addition of rational points on a chosen elliptic curve, and the number of rational points is uniquely determined on the elliptic curve. If we define the s scalar multiplication of a point P as the operation by which point P is added to itself s times, i.e. the resulting point sP, one important property is that it is computationally difficult to find an integer s from points Q and P such that $Q = sP$ by a polynomial time-bounded algorithm. This problem is called “the discrete logarithm problem over the

elliptic curve" a.k.a. ECDLP. Thus the security of ECC is based upon the difficulty of solving the problem [44][45] and [46].

2.2 Proxy Blind Signature Based on ECDLP

A proxy blind signature is a digital signature scheme that performs the functions of both proxy signature and blind signature schemes. Usually a proxy blind signature scheme involves three parties: the original signer, the proxy signer and the verifier. Each participant has a pair of cryptographic keys that are generated over elliptic curve cryptography. The proxy blind signature scheme typically consists of the following phases [24][26][27] and [28]:

- *Proxy delegation phase:* The phase of proxy delegation takes input the system arguments (e.g., $R_O = k_O \cdot P = (x_1, y_1)$, $r_O = x_1 \bmod n$, $s_O = x_O + k_O \cdot H(m_w \| r_O) \bmod n$) from the original signer and creates a corresponding proxy credential (e.g., (R_O, s_O, m_w)) as output. The original signer sends the proxy generation with the delegation of authority to the proxy signer through a secure channel. Having received the proxy delegation, the proxy signer checks the validity of the authorized message with a specific type of authentication (e.g., $s_O \cdot P = R_O \cdot H(m_w \| r_O) + y_O$).
- *Blind signature phase:* The procedure of blind signature takes as input a proxy delegation, the secret arguments (e.g., $R_P = k_P \cdot P = (x_2, y_2)$, $r_P = x_2 \bmod n$) from the proxy signer and outputs a cryptogram data (e.g., (R_O, R_P, m_w)) such as the warrant message and the corresponding identities of the original and the proxy signers. The coded message will be delivered to the verifier from the proxy signer. The verifier embeds certain blinding factors in the blinded message (e.g., $R^* = R_P + b \cdot P - Y_{pr}(a + c)$, $e^* = H(R^* \| m) \bmod n$, $e = e^* - c - a \bmod n$) and the resulting message is passed to the proxy signer. Upon receiving the blinded message, the proxy signer signs it (e.g., $S'' = e \cdot S_{pr} + k_P \bmod n$) and then sends the proxy blind signature back to the verifier.
- *Verification phase:* The stage of verification takes input the signature-message tuple (e.g., m_w, r_O, m, e^*, S) from the proxy signer and verifies a valid proxy blind signature as output. The verifier extracts the proxy blind signature from eliminating the blinding factors and checks the validity of the proxy blind signature by a proper verification process (e.g., $e^* = H((SP - e^* \cdot Y_{pr}) \| m)$.

3. The Proposed Scheme

In this section, we propose a secure and efficient proxy blind signcryption scheme for a single digital message or multiple electronic message contents based on the difficulty of the ECDLP. Solving the underlying computationally hard problem is currently considered infeasible if a dishonest adversary attempts to collect some secret information from designated proxy signers to perform the stipulated task (e.g. counterfeit a proxy signature). In addition, the shift permutation mechanism is incorporated into our scheme to raise the levels of security for the transmission of such information. Combined with the interleaving structural designs, this work has certainly yielded promising results on the improvements of security and efficiency. The proposed scheme comprises the following three stages: proxy delegation stage, blind signcryption stage and verification stage.

The operational context diagram of the proposed scheme is shown in **Fig. 1**, and **Table 1** lists the symbols and the denotations thereof about the approach used. There are three kinds of roles in our proxy blind signcryption scheme, namely an original signer *O*, a proxy signer *P* and a requester *D* respectively. Also, in order to help untangle the concept of complexity

examining the method, a control server that acts as an intermediary for each member requisition performs tasks such as initialization, registration and authentication.

In the initialization assignment, the server selects a secure elliptic curve $E(F_q)$ that is defined over a finite field F_q, and picks a base point $G = (x_1, y_1) \in E(F_q)$ whose order is a positive integer n such that $n \cdot G = \infty$. Meanwhile, the server computes its public key PK_{Server}, mathematically derived from a given private key sk_{Server}. Then, the specific configuration settings (e.g., $E(F_q)$, G, n, PK_{Server}, $h_1()$, $h_2()$, $h_3()$, $h_4()$, $f_1()$ and $f_2()$) are applied to all users on a public network. During the registration period, it is necessary to provide each user identification data as well as all of the associated information for acquiring the server issued certificate or signature. While every signed-in user has successfully passed the registration process, all legitimate members are always permitted to use the services available through the server. As for the authentication procedure, in order to make registered users communicate over the network properly and effectively, performing a mutual authentication that proves their respective identities to each other is required prior to message exchange and information transmission.

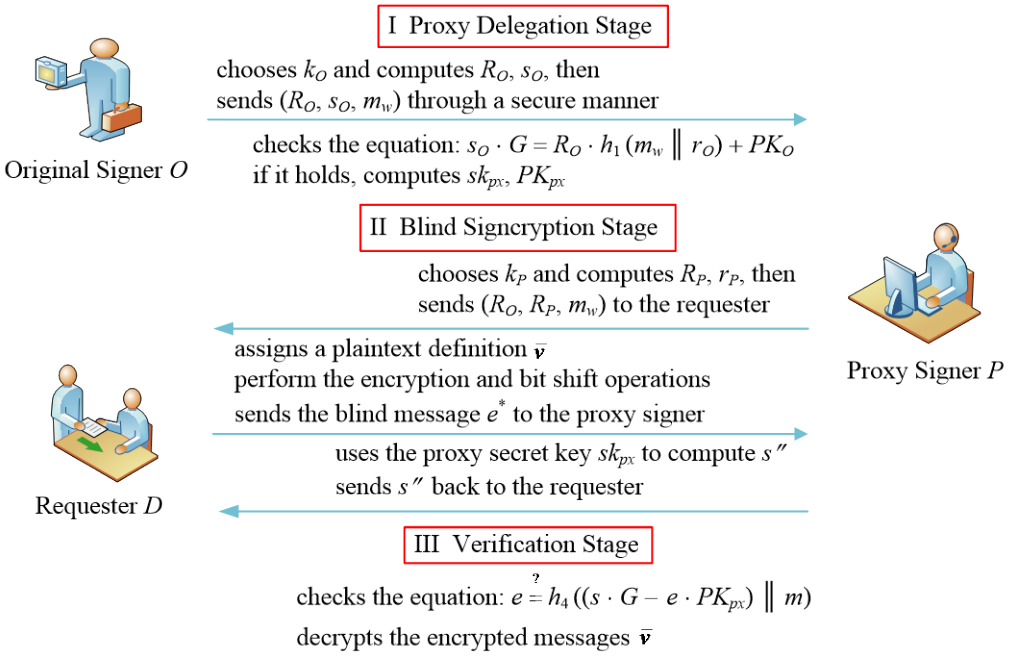

Fig. 1. The operational context diagram of the proposed scheme

Table 1. The system parameters and the explanations

Item	Symbol	Description
1	$E(F_q)$	an elliptic curve E over a finite field F_q
2	G	a base point G of an elliptic curve
3	n	an order n of an elliptic curve
4	q	a large prime number q such that $q > 2^{283}$
5	PK_O, PK_P, PK_D	public keys of an original signer O, a proxy signer P, and a requester D
6	sk_O, sk_P, sk_D	private keys of an original signer O, a proxy signer P, and a requester D
7	k_O, k_P, k_D	randomly selected values by an original signer O, a proxy signer P, and a requester D

8	$h_1(\ )$	a hash function for values transposition
9	$h_2(\ )$	a hash function for plaintext blocks transposition
10	$h_3(\ )$	a hash function for a series of ciphertext points transposition
11	$h_4(\ )$	a hash function for points transposition
12	$f_1(\ )$	a function that transforms a message into a point on an elliptic curve
13	$f_2(\ )$	a function that converts a point into a message on an elliptic curve
14	V	a plaintext message
15	C	a ciphertext form
16	w	a knapsack sequence of either 0 or 1 in plaintext
17	t	a hash value of a plaintext sequence
18	m	a signed message digest
19	m_w	a proxy warrant
20	$\|\|$	the concatenation operation

3.1 Proxy Delegation Stage

This stage comprises mainly three, a proxy generation step, a proxy delivery step, and a proxy verification step.

- The original signer O first selects a random number $k_O \in [2, n-1]$ and calculates $R_O = k_O \cdot G = (x_1, y_1)$, $r_O = x_1 \bmod n$, and $s_O = sk_O + k_O \cdot h_1(m_w \| R_O) \bmod n$ as the secret parameters.
- Next, the original signer O delivers (R_O, s_O, m_w) to the proxy signer P using a secure channel.
- While receiving the dataset (R_O, s_O, m_w), the proxy signer P then checks the validity of the data message with the following equation (1).

$$s_O \cdot G = R_O \cdot h_1(m_w \| r_O) + PK_O \tag{1}$$

- If the two sides of the equation are equal to each other, the proxy signer P accepts the delegated request from the original signer O, and computes the proxy secret key sk_{px} and the corresponding proxy public key PK_{px}, respectively by using equations (2) and (3).

$$sk_{px} = sk_P + s_O \bmod n \tag{2}$$

$$PK_{px} = PK_O + PK_P + R_O \cdot h_1(m_w \| r_O) = sk_{px} \cdot G \tag{3}$$

3.2 Blind Signcryption Stage

When the proxy delegation has been expressly designated, the proxy signer P and the requester D will do the following steps to blindly signcrypt the message m. We state the blind signcryption procedure below.

- First of all, the proxy signer P chooses a random number $k_P \in [2, n-1]$, and computes $R_P = k_P \cdot G = (x_2, y_2)$ and $r_P = x_2 \bmod n$. Then, the covert message (R_O, R_P, m_w) is sent to the requester D.
- Second, the requester D divides a message into several data blocks as the form of $\bar{v} = \{v_1, v_2, \ldots, v_i\}\ (i \geq 1)$, and uses equation (4) to generate a hash value t. Additionally, equation (5) is applied to carry out the transformation of data blocks v_i to elliptic curve points V_i.

$$h_2(\bar{v}) = t \tag{4}$$

$$f_1(\bar{v}) = \{V_1, V_2, \ldots, V_i\} \tag{5}$$

- And then, the requester *D* defines a binary string that has the form $\bar{p} = \{p_1, p_2, \ldots, p_i\}$ such that each digit is either 0 or 1, and lets each entry p_i in the sequence of binary bits match exactly the number of the data points V_i. Afterwards, the requester *D* generates a random number, *w*, as a permutation value, and the given decimal integer will be converted into its binary form, w_1 w_2, ..., w_i, so as to map elements of the set of $\bar{p}$. The binary string is then scrambled iteratively using two consecutive bits and finally shifted at the bit-level permutation. The permutation encoding of control bits w_i starts with the most significant bit and moves towards the least significant bit. The working principle underlying the bitwise operation is essentially represented by the construction of logical expressions as follows. When the current binary digit is 1 and the next digit is 0, a right shift (>>) of one bit position is performed to the corresponding data points V_i. The shifting right (>>) by three bits, which shifts the relevant point three positions to the right, is decided if the two consecutive bits are equal to 1. Similarly, if the current bit at position is 0 and the next bit is 1, a left shift (<<) is used to move this data point to the left one position. The operation (<<) shifts three bits in a variable toward the left when there is the occurrence of two consecutive zeros on the bit pattern of the data points.
- Next, the requester *D* finds an intractable point *K* as it is computed by equation (6), and then selects other necessary parameters including an arbitrary positive integer *w*, a hash value *t*, a random elliptic curve element *k* and the public key PK_P from the proxy signer *P*, to systematically convert the plaintext elements into the corresponding positions of ciphertext points according to equations (7) and (8). In this way, each succeeding ciphertext block is sequentially incorporated into the preceding ciphertext block until they are chained together to form a continuous encoded message $\bar{C} = \{C_0, C_1, C_2, \ldots, C_i\}$. When the transposition cipher has been successfully implemented, the requester *D* makes use of equation (9) to create a hash-based value *m*.

$$K = k \cdot G \tag{6}$$

$$C_0 = [f_1(w,t) + k \cdot PK_P] \tag{7}$$

$$C_i = [V_i + p_i \cdot C_{i-1}], 1 \le i \le n \tag{8}$$

$$h_3(\bar{C}) = m \tag{9}$$

- After that, the requester *D* randomly chooses three blinding factors *a*, *b*, and *c*, to arrange a secret point *R* as expressed in equation (10). If the secret point *R* is equivalent to the point at infinity ∞ on the elliptic curve, the requester *D* seeks out another secret point with a different 3-tuple (*a*, *b*, *c*) until $R \neq \infty$. After the secret point *R* has been discovered, the requester *D* then blinds the message *m* by using equations (11) and (12), and sends the blinded message to the proxy signer *P*.

$$R = a \cdot R_P + c \cdot G - b \cdot PK_{px} \tag{10}$$

$$e = h_4(R \| m) \bmod n \tag{11}$$

$$e^* = a^{-1}(e - b) \bmod n \tag{12}$$

- Then, upon receiving the blinded message e^* the proxy signer P uses the proxy secret key sk_{px} and an arbitrary number k_P to produce the blind signature s'' defined by equation (13), and sends it back to the requester D.

$$s'' = e^* \cdot sk_{px} + k_P \bmod n \tag{13}$$

- Finally, the requester D applies the blind signature s'' to equation (14), to remove the blinding factors (a, b and c) for the purpose of revealing the unblinded signature value s. Now, the message-signature tuple has the form (m_w, R_O, m, e, s, $\overline{C}$, K).

$$s = a \cdot s'' + c \bmod n \tag{14}$$

3.3 Verification Stage

The verification stage is a two-step progress on the signed message, based on the validation of the proxy blind signature value s and the restoration of the encrypted message $\overline{C}$.

- To begin with, the requester D uses the proxy signer's public key PK_{px} and the blinded message digest e to verify the legitimacy of the signature value by checking whether there exists a solution to equation (15). If the message digest matches the received content of all corresponding parameters, the signature value s is deemed valid and the requester D is able to proceed to the decryption step.

$$\overset{?}{e} = h_4((s \cdot G - e \cdot PK_{px}) \,||\, m) \tag{15}$$

- Next, the requester D takes the initial encoded data block C_0 of the ciphertext message $\overline{C}$, the private key sk_D and the particular point K as input measures to unwrap the pair of untransformed data (w, t) by applying the two conversion functions $f_1(\ )$ and $f_2(\ )$ described in equations (16) and (17).

$$f_1(w, t) = C_0 - sk_D \cdot K \tag{16}$$

$$(w, t) = f_2[f_1(w, t)] \tag{17}$$

- In addition, once the crucial message component (w, t) is obtained, the requester D can investigate the permutation sequence w in binary format to the corresponding message sequence $\overline{p}$ as a previously defined form, and performs the inverse bit-shifting operations on such binary representations to find the message sequence of the items associated with the positions. Each item p_i projected onto the data point V_i is then mapped to the shifting position given by this permutation value w_i. That is, the result of repeatedly applying the right shift (>>) by one position to a given pair of bit values if the bit at the current position is 0 and the next bit position is 1. If two consecutive bits are 0, the result of performing a three position right shift (>>) on the pattern is obtained. Correspondingly, shifting this bit pattern to the left one position (<<) is carried out when the current bit at position is 1 and the next low-order bit is 0. If its two successive bits in the compared position are 1, the data points will be shifted left (<<) by 3 positions. While the series of bit permutations w_i is interpreted as the sequence of the block ciphers C_i

associated with the position, the requester D methodically reverts the ciphertext message $\overline{C} = \{C_0, C_1, C_2, \ldots, C_i\}$ that depends on the current and the immediately preceding ciphertext block, to the plaintext segments of elliptic curve data points as indicated by equation (18).

$$V_i = [C_i - p_i \cdot C_{i-1}], 1 \le i \le n \tag{18}$$

- Finally, when the collection of the elliptic curve data points in making up the plaintext segments is complete as the form of equation (19), the requester D uses the conversion function $f_2(\,)$ again as expressed in equation (20), to turn the mapping data points into the representations of numeric values. All the split segments in the sequence are then concatenated to form a related text message, and the original plaintext is exactly recovered.

$$\overline{V} = \{V_1, V_2, \ldots, V_i\} \tag{19}$$

$$f_2(\overline{V}) = \overline{v} \tag{20}$$

3.4 Correctness of the Proposed Scheme

The correctness of the proposed scheme can be verified by examining if the equation $h_4(s \cdot G - e^* \cdot PK_{px} \| m) = h_4(R \| m)$ holds. That is, anyone with the proxy signer's public key PK_{px} can check the correctness of a blind signature s. We prove its correctness as follows.

$$\begin{aligned}
& s \cdot G - e \cdot PK_{px} \\
&= (a \cdot s'') \cdot G - e \cdot PK_{px} \\
&= (e^* \cdot sk_{px} + k_P)\, a \cdot G + c \cdot G - e \cdot PK_{px} \\
&= e^* \cdot sk_{px} \cdot a \cdot G + k_P \cdot a \cdot G + c \cdot G - e \cdot PK_{px} \\
&= a \cdot PK_{px} \cdot a^{-1}(e - b) + a \cdot R_P + c \cdot G - e \cdot PK_{px} \\
&= a \cdot PK_{px} - b \cdot PK_{px} + a \cdot R_P + c \cdot G - e \cdot PK_{px} \\
&= a \cdot R_P + c \cdot G - b \cdot PK_{px} \\
&= R
\end{aligned}$$

4. Security Analysis of the Proxy Blind Signcryption Scheme

The security of the new proposed approach is based upon the difficulty of solving the ECDLP. Also, the signcryption method is incorporated into the proposed algorithm for the duration of a blind signature construction. On the basis of these two techniques, our scheme satisfies the security requirements under the hardness of the ECDLP and the verification of the blind signcrypted messages by any proxy delegation. Besides providing the essential properties of blind signature, namely unforgeability and unlinkability (or blindness) [4][5], the proposed scheme conforms to the security characteristics of proxy signature in confidentiality, distinguishability, identifiability, verifiability, non-repudiation and prevention of misuse [26][28][29] and [47]. These security goals of our approach are investigated as follows.

4.1 Unforgeability

Unforgeability refers that no one is able to forge a valid proxy blind signature on any arbitrary message aside from the designated proxy signer. In the proposed protocol, if an adversary tries to determine the possible values in the delegation message-signature tuple of (m_w, R_O, m, e, s, $\overline{C}$, K) from the public channel, he/she cannot derive the proxy blind signature, s, from the given proxy public key PK_{px}. It is computationally infeasible for the adversary to compute s without the proxy secret key sk_{px}, and he/she is unable to pass the verification measure $e \stackrel{?}{=} h_4((s \cdot G - e \cdot PK_{px}) \| m)$ by equation (15).

4.2 Unlinkability

Unlinkability means that the proxy signer cannot adequately distinguish whether the blinded message and the proxy blind signature are related or not. The blinded message of our scheme is generated by equation (12) as $e^* = a^{-1}(e - b) \bmod n$ and the proxy signer P has knowledge of (m_w, R_O, m, e^*, s'', R_P, $\overline{C}$, K). The proxy signer P or an attacker is unable to obtain the blinded message e^* without the blinding factor (a, b, c), and fails to find the relationship between (m_w, R_O, m, e, s, $\overline{C}$, K) and (R, e^*, s''). Finding the blinding factors in equation (10) leads to encounter calculating the number of points on the elliptic curve over fields, and it becomes extremely difficult to break the value of knowing desired points when tackling the ECDLP. The second hard thing is not an easy attempt that reverses a one-way hashing function described by equation (11).

4.3 Confidentiality

Confidentiality prevents the unauthorized use or disclosure of the proxy blind signcryption information, ensuring that only those who have legitimate access can do so. In the design of a proxy blind signcryption mechanism, all plaintext first is permuted and blinded by the requester D, signcrypted by the proxy signer P, and then got processed by elliptic curve arithmetic operations before sending the proxy blind signcrypted message back to the requester D. If any adversary intercepts the transmitted message from a past communication, the interceptor is unable to easily compromise the encrypted session because he/she does not know a long list of secret parameters, such as (R_O, R_P, m_w, m, e^*, s'', sk_D, $\overline{C}$, K), on the blind signcryption text. It is significantly hard to decrypt the resulting message when many other factors have to be taken into consideration.

4.4 Distinguishability

Distinguishability specifies that the proxy blind signature must be capable of being perceived as distinct from the general signature. In this study, the blind signcrypted information (m_w, R_O, m, e, s, $\overline{C}$, K) involves the proxy warrant m_w from the original signer O, which allows a delegate the ability to sign messages and the secret parameter is conveyed to the proxy signer P. Therefore, the proxy blind signature is easily distinguishable from the ordinary signature.

4.5 Identifiability

Identifiability indicates that anyone can determine the identities of the original signer and the proxy signer from the proxy blind signature data. In our design, the proxy public key PK_{px} is established by using equation (3) $PK_{px} = PK_O + PK_P + R_O \cdot h_1(m_w \| r_O)$ containing both the original signer's public key PK_O and the proxy signer's public key PK_P. Furthermore, the blind

signcrypted message (m_w, R_O, m, e, s, $\overline{C}$, K) is recognized by the verification equation $e \stackrel{?}{=} h_4((s \cdot G - e \cdot PK_{px}) \| m)$. Hence, the requester D or any user can successfully achieve the identity authentication from the proxy blind signcrypted information.

4.6 Verifiability

Verifiability denotes that the proxy blind signature information can be verified by anyone and a signature receiver can be convinced that the signed message has been delegated to a proxy signer by the original signer to whom it was assigned. In this scheme, the blind signcrypted message (m_w, R_O, m, e, s, $\overline{C}$, K) can be approved to the requester D or anybody since the proxy signer P has the proxy warrant m_w created by the original signer O. Likewise, the warrant certificate comprises the information regarding the original signer's identity, the proxy signer's identity, the relative rights, etc. Thus, requester D is able to ensure the original signer's agreement on the blind signcrypted message.

4.7 Non-repudiation

Non-repudiation implies that the original signer and the proxy signer cannot deny the authenticity of their signatures on the sending message that they originated from. In our case, the proxy secret key sk_{px} is expressed by equation (2) as $sk_{px} = sk_P + s_O \bmod n$, and only the proxy signer P knows sk_{px} if sk_P is owned by P. And the original signer O must have a particular secret key sk_O and uniquely know s_O by the equation $s_O = sk_O + k_O h_1(m_w \| R_O) \bmod n$. Neither the proxy signer P nor the original signer O can learn anything about the portion of the shared session key from each other. So, both the original signer and the proxy signer are unable to repudiate having signed on the blind signcrypted message.

4.8 Prevention of Misuse

Prevention of misuse suggests that the proxy signer cannot use the proxy key pair for intentions other than creating a valid proxy signature in compliance with the delegation information. The proxy warrant m_w of the proposed scheme is issued by the original signer O authorizing the proxy signer P to sign messages on behalf of him/her, and the limits of the designated signcrypted authority is clearly specified when such a delegation is specially authorized. Moreover, the proxy key pair (PK_{px}, sk_{px}) is generated in a secure manner through two equations (2) and (3) and they are uniquely related each other's keys. In case of misuse, the proxy signer P cannot blindly signcrypt message unless authorized to do so by the original signer O.

We have inspected the security characteristics of the proposed scheme in terms of a proxy blind signcryption program, and the safeguard mechanism completely accords with the security attributes for the implementation of both blind signatures and proxy signatures. If we re-examine the similarity models of the existing proxy blind signature (or signcryption) methods by comparing the security level, it is obvious that our scheme provides for effective countermeasures in security considerations, such as Tan et al.'s scheme [20] has been pointed out that it may be subject to a forged signatures issue, Yang and Yu's method [24] does not satisfy the property of unforgeability, Alghazzawi et al.'s algorithm [27] doesn't provide ciphertext unlinkability, Wang and Liao's approach [28] might cause confidential information to be disclosed, and Sadat et al.'s solution [29] only aims at blinding or disguising messages and does not yield data confidentiality to strengthen the secrecy of information. By comparison with the existing techniques for proxy blind-signature or blind-signcryption purposes, the proposed scheme is able to fulfill all the security properties as claimed. **Table 2**

presents a comparison between our scheme and the above-mentioned five existing proposals along with the corresponding proxy blind signature (or signcryption) techniques. The symbol, √, is interpreted to mean that it is satisfied if the security feature identifier is supported, whereas the symbol, ×, is specified to indicate if the proposal does not place the appropriate evidence of that satisfaction on the security capability. As depicted in **Table 2**, the recommended solution addresses all aspects of the security policy at both the blind and proxy signatures, while the existing approaches suffer from some essential weaknesses such as unforgeability, unlinkability, confidentiality, identifiability and prevention of misuse.

Table 2. Comparative analysis of the proposed scheme with other existing methods in terms of security measures

Algorithm / Security capabilities	Tan et al.'s scheme [20]	Yang et al.'s scheme [24]	Alghazzawi et al.'s scheme [27]	Wang et al.'s scheme [28]	Sadat et al.'s scheme [29]	Our scheme
Unforgeability	×	×	√	√	√	√
Unlinkability	×	√	×	√	×	√
Confidentiality	×	×	×	×	√	√
Distinguishability	√	√	√	√	√	√
Identifiability	√	√	√	√	×	√
Verifiability	√	√	√	√	√	√
Non-repudiation	√	√	√	√	√	√
Prevention of misuse	×	√	√	√	√	√

Note: The basic security criteria of a blind signature protocol must satisfy the unforgeability and unlinkability properties, while a signcryption scheme should simultaneously provide confidentiality protection.

5. Performance Evaluation of the Proposed Protocol

Having described the relevant security assessment of our protocol, we evaluate the performance of the proposed scheme, and then show that it brings great efficiency with respect to the application of proxy blind signature systems by comparison to other existing methods. We will examine the theoretical frameworks of these different suggestions for solving the cryptological techniques related to the computation and communication costs incurred by each task in accordance with the concept of modular arithmetic operations [38][48] and [49]. The computational operations and key symbols, including scalar multiplication, point addition, hash construction and modular arithmetic, are shown in **Table 3**.

Table 3. The modular mathematical notation

Symbol	Arithmetic operation	Estimated cost
T_{MUL}	the time for the modular multiplicative operation	$= 1T_{MUL}$
T_{EXP}	the time for the modular exponential operation	$\approx 240T_{MUL}$
T_{ADD}	the time for the modular addition operation	(negligible execution time)
T_{INVS}	the time for the modular multiplicative inverse operation	$\approx 240T_{MUL}$
T_{ECMUL}	the time for the multiplicative operation of an elliptic curve point	$\approx 29T_{MUL}$

T_{ECADD}	the time for the addition operation of two points on an elliptic curve	$\approx 5T_{MUL}$
T_h	the time for the operation of a map-to-point hash function on an elliptic curve	$\approx 23T_{MUL}$
t_h	the time for the operation of a conventional hash function	$\approx 0.4T_{MUL}$

The notation description enables us to summarize the computational costs of each step involved in these proxy blind signature (or signcryption) models as presented in **Table 4**. Compared to the other related algorithms for performing one single message processing, it turns out that the proposed scheme executes two more required operations every time, thus creating a performance penalty for encryption and decryption actions. Dealing with the operations, for example, that map a message block or an integer to an elliptic curve point and vice versa, is consequently time consuming. With additional advanced protections, each task helps information communication to defend against the cyber threats while some of the existing technologies may incur malicious attacks due to the lack of confidentiality capability. However, if we compare the results with the same baseline measures (i.e., without the tradeoffs of encryption-and-decryption implementation cost), the efficiency of the proposed solution is significantly improved over most of the existing approaches, and its computational cost is approximately $536T_{MUL}$.

Table 4. Performance comparison between the proposed scheme and the existing algorithms for one single message processing

Stage / Cost / Method		Tan et al.'s scheme [20]	Yang al.'s scheme [24]	Alghazzawi et al.'s scheme [27]	Wang et al.'s scheme [28]	Sadat et al.'s scheme [29]	Our scheme
Proxy delegation	Proxy	$3T_{ECMUL}+1T_{ECADD}+1T_{MUL}+2T_{ADD}\approx 93T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}+1T_{MUL}+2T_{ADD}\approx 64T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}+1T_{MUL}+1T_{ADD}\approx 64T_{MUL}$	$3T_{ECMUL}+3T_{ECADD}+1T_{MUL}+2T_{ADD}+3t_h\approx 104T_{MUL}$	$3T_{ECMUL}+1T_{ECADD}+2T_{MUL}+1T_{ADD}+3t_h\approx 95T_{MUL}$	$3T_{ECMUL}+3T_{ECADD}+1T_{MUL}+2T_{ADD}+3t_h\approx 104T_{MUL}$
Blind signcryption	Encryption	None	None	None	None	Not elaborated much on the step	$2T_{ECMUL}+1T_{ECADD}+1T_h+1t_h\approx 86T_{MUL}$
	Blind Signature	$8T_{ECMUL}+6T_{ECADD}+3T_{MUL}+7T_{ADD}+1t_h\approx 265T_{MUL}$	$5T_{ECMUL}+3T_{ECADD}+4T_{MUL}+2T_{ADD}+1T_{INVS}+1t_h\approx 404T_{MUL}$	$3T_{ECMUL}+2T_{ECADD}+2T_{MUL}+3T_{ADD}+1t_h\approx 99T_{MUL}$	$4T_{ECMUL}+2T_{ECADD}+3T_{MUL}+3T_{ADD}+1T_{INVS}+1t_h\approx 369T_{MUL}$	$4T_{ECMUL}+2T_{ECADD}+1T_{MUL}+4T_{ADD}+1T_{INVS}\approx 367T_{MUL}$	$4T_{ECMUL}+2T_{ECADD}+3T_{MUL}+3T_{ADD}+1T_{INVS}+1t_h\approx 369T_{MUL}$
Verification	Verification	$3T_{ECMUL}+3T_{ECADD}+1t_h\approx 102T_{MUL}$	$2T_{ECMUL}+3T_{ECADD}+1t_h\approx 73T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}+1T_{MUL}+1t_h\approx 64T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}+1t_h\approx 63T_{MUL}$	$3T_{ECMUL}+2T_{ECADD}+1t_h\approx 97T_{MUL}$	$2T_{ECMUL}+1T_{ECADD}+1t_h\approx 63T_{MUL}$
	Decryption	None	None	None	None	Not elaborated much on the step	$2T_{ECMUL}+2T_{ECADD}\approx 68T_{MUL}$
Total cost without encryption and decryption		$\approx 460T_{MUL}$	$\approx 541T_{MUL}$	$\approx 227T_{MUL}$	$\approx 536T_{MUL}$	$\approx 559T_{MUL}$	$\approx 536T_{MUL}$
Total cost with encryption and decryption		$\approx 460T_{MUL}$	$\approx 541T_{MUL}$	$\approx 227T_{MUL}$	$\approx 536T_{MUL}$	$\approx 559T_{MUL}$	$\approx 690T_{MUL}$

As the number of digital messages (e.g., a multi-page electronic document) has been gradually increasing, the existing protocols will often step through each of the operations in turn by iterating multiple times, whereas the proposed scheme only needs one time to perform the three-stage procedure for establishing proxy blind signcryption. Since an incremental volume of digital messages among points specified by the individual is taken into consideration, maintaining the transmission efficiency of proxy blind signature (or signcryption) protocols becomes a critical part of the effort as well as security requirements. To estimate the composition performance levels for these proxy blind signature or signcryption schemes by running on its processing the digital messages multiple times, we repeatedly apply the necessary steps to carry out each identified cryptographic operation. As shown in **Table 5**, the existing schemes explicitly cause a substantial increase in the computational costs for managing the vast amount of digital messages in number of up to 3 units, while the proposed protocol provides efficient operations without increasing the computational time significantly. Unlike the previous approaches to the task of cryptographic-related operations in working on a large number of digital messages, the proposed scheme requires only one time process to perform the three steps of proxy delegation, blind signcryption and verification, rather than goes through the design process of repeating the various stages several times. Similarly, **Fig. 2** shows that our computational cost remains unchanged and is still the same in handling large numbers of digital messages, but the existing methods become faster and steeper growth of the total cost.

Table 5. Comparison of efficiency between the proposed scheme and other approaches regarding multiple digital messages processing

Algorithm / Number of digital messages	Tan et al.'s scheme [20]	Yang et al.'s scheme [24]	Alghazzawi et al.'s scheme [27]	Wang et al.'s scheme [28]	Sadat et al.'s scheme [29]	Our scheme
1	$\approx 460T_{MUL}$	$\approx 541T_{MUL}$	$\approx 227T_{MUL}$	$\approx 536T_{MUL}$	$\approx 559T_{MUL}$	$\approx 536T_{MUL}$
2	$\approx 920T_{MUL}$	$\approx 1082T_{MUL}$	$\approx 454T_{MUL}$	$\approx 1072T_{MUL}$	$\approx 1118T_{MUL}$	$\approx 536T_{MUL}$
3	$\approx 1380T_{MUL}$	$\approx 1623T_{MUL}$	$\approx 681T_{MUL}$	$\approx 1608T_{MUL}$	$\approx 1677T_{MUL}$	$\approx 536T_{MUL}$
4	$\approx 1840T_{MUL}$	$\approx 2164T_{MUL}$	$\approx 908T_{MUL}$	$\approx 2144T_{MUL}$	$\approx 2236T_{MUL}$	$\approx 536T_{MUL}$
5	$\approx 2300T_{MUL}$	$\approx 2705T_{MUL}$	$\approx 1135T_{MUL}$	$\approx 2680T_{MUL}$	$\approx 2795T_{MUL}$	$\approx 536T_{MUL}$

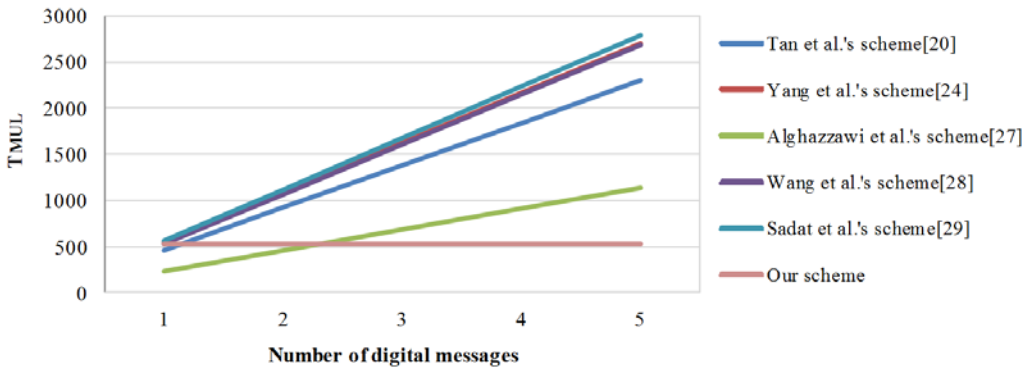

Fig. 2. Schematic diagram of between the multiplicative cost consumption and their respective processes for the number of digital messages

According to the graphical and tabular summarization, we believe that the proposed model has superior performance in carrying out different cryptographic operations on a large number of digital messages compared with other recommended algorithms in accordance with fulfilling the communication request. With this kind of promptness, the suggested scheme is much more efficient for usage in various proxy blind signature or signcryption applications this way.

6. Conclusions

We have presented a new proxy blind signcryption scheme by coming up with the countermeasure for multiple digital messages processing based on the ECDLP difficulty. To enhance the security of messages signed on behalf of the original signer as the proxy is printed, having the signcryption-permutation technique along with the cryptographic primitives is thoroughly incorporated into the proxy blind signature function. The additional characteristics of the cryptosystem make the corresponding proxy signature procedure more efficient and secure, meanwhile it protects the transfer of the signed message from security threats such as identity, privacy and unauthorized access.

This paper has also described how the combined concepts of encryption and blind signcryption can help develop a proxy blind signcryption protocol, indicating that the proposed scheme is capable of having the benefits of processing multiple proxy blind signcrypted information in both security and efficiency compared to the other existing solutions. Through the security analysis, the study achieves all of the related security requirements for a proxy blind signature system in Section 4. Moreover, in a comparative study for coping with large numbers of digital messages the work reveals the superiority of the anticipated effects on performance evaluation, and the experimental results show that this scheme has less overhead complexity than its elliptic-curve based variants, as presented in Section 5. From the above-mentioned characteristics, we are convinced that the current scheme provides significant ameliorations with high security settings and low communication overheads for proxy blind signatures and their applications, such as e-voting, e-cash and e-commerce systems, and this model is very beneficial particularly in mobile computing environments when these devices may have limited communication capabilities and power supplies.

References

[1] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology – CRYPTO'82*, *Lecture Notes in Computer Science*, Springer, vol. 3, pp. 199-203, 1983. Article (CrossRef Link).

[2] M. S. Hwang, C. C. Lee and Y. C. Lai, "An untraceable blind signature scheme," *IEICE Transactions on Foundations*, vol. E86-A, no. 7, pp. 1902-1906, 2003.

[3] O. Blazy, G. Fuchsbauer, D. Pointcheval and D. Vergnaud, "Short blind signatures," *Journal of Computer Security*, vol. 21, no. 5, pp. 627-661, 2013. Article (CrossRef Link).

[4] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," *Journal of Cryptology*, vol. 13, no. 3, pp. 361-396, 2000. Article (CrossRef Link).

[5] N. M. F. Tahat, E. S. Ismail and R. R. Ahmad, "A new blind signature scheme based on factoring and discrete logarithms," *International Journal of Cryptology Research*, vol. 1, no. 1, pp. 1-9, 2009.

[6] I. Lin, M. Hwang and C. Chang, "Security enhancement for anonymous secure e-voting over a network," *Computer Standards and Interfaces*, vol. 25, no. 2, pp. 131-139, 2003. Article (CrossRef Link).

[7] J. H. Wang, J. W. Liu, X. H. Li and W. D. Kou, "Fair e-payment protocol based on blind signature," *Journal of China Universities of Posts and Telecommunications*, vol. 16, no. 5, pp. 114-118, 2009. Article (CrossRef Link).
[8] D. Yong, L. Bin and Z. Zhaoxia, "An electronic auction scheme based on group signatures and partially blind signatures," *Procedia Engineering*, vol. 15, pp. 3051-3057, 2011. Article (CrossRef Link).
[9] J. Leiwo, C. Hanle, P. Homburg and A. S. Tanenbaum, "Disallowing unauthorized state changes of distributed shared objects," *Information Security for Global Information Infrastructures*, vol. 47, Springer-Verlag, pp. 381-390, 2000. Article (CrossRef Link).
[10] H. U. Park and I. Y. Lee, "A digital nominative proxy signature scheme for mobile communication," *Lecture Notes in Computer Science*, Springer-Verlag, vol. 2229, pp. 451-455, 2001. Article (CrossRef Link).
[11] M. A. Jabri and S. Matsuoka, "Authorization within grid-computing using certificateless identity-based proxy signature," in *Proc. of the 19th ACM International Symposium on High Performance Distributed Computing*, pp. 292-295, 2010. Article (CrossRef Link).
[12] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures: delegation of the power to sign messages," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E79-A, no. 9, pp. 1338-1353, 1996.
[13] H. M. Sun, "Design of time-stamped proxy signatures with traceable receivers," *IEE Proceedings - Computers and Digital Techniques*, vol. 147, no. 6, pp. 462-466, 2000. Article (CrossRef Link).
[14] E. J. L. Lu, M. S. Hwang and C. J. Huang, "A new proxy signature scheme with revocation," *Applied Mathematics and Computation*, vol. 161, no. 3, pp. 799-806, 2005. Article (CrossRef Link).
[15] Y. S. Kim and J. H. Chang, "Self proxy signature scheme," *International Journal of Computer Science and Network Security*, vol. 7, no. 2, pp. 335-338, 2007.
[16] N. R. Sunitha and B. B. Amberker, "Proxy signature schemes for controlled delegation," *Journal of Information Assurance and Security*, vol. 3, no. 2, pp. 159-174, 2008.
[17] H. Y. Lin, T. S. Wu and S. K. Huang, "An efficient strong designated verifier proxy signature scheme for electronic commerce," *Journal of Information Science and Engineering*, vol. 28, no. 4, pp. 771-785, 2012. Article (CrossRef Link).
[18] L. Pang, H. Zhao, X. Zhou and H. Li, "Strongly unforgeable and efficient proxy signature scheme with fast revocation secure in the standard model," *International Journal of Distributed Sensor Networks*, vol. 2016, pp. 1-12, 2016. Article (CrossRef Link).
[19] W. D. Lin and J. K. Jan, "A security personal learning tools using a proxy blind signature scheme," *Proceedings of International Conference on Chinese Language Computing*, pp. 273-277, 2000.
[20] Z. Tan, Z. Liu and C. Tang, "Digital proxy blind signature schemes based on DLP and ECDLP," *MM Research Preprints, MMRC, AMSS, Academia*, vol. 21, pp. 212-217, 2002.
[21] A. K. Awasthi and S. Lal, "Proxy blind signature scheme," *Transaction on Cryptology*, vol. 2, no. 1, pp. 5-11, 2005.
[22] H. M. Sun, B. T. Hsieh and S. M. Tseng, "On the security of some proxy blind signature schemes," *Journal of Systems and Software*, vol. 74, no. 3, pp. 297-302, 2005. Article (CrossRef Link).
[23] H. Y. Wang and R. C. Wang, "A proxy blind signature scheme based on ECDLP," *Chinese Journal of Electronics*, vol. 14, no. 2, pp. 281-284, 2005.
[24] X. Yang and Z. Yu, "Security analysis of a proxy blind signature scheme based on ECDLP," in *Proc. of the 4th International Conference on Wireless Communications, Networking and Mobile Computing* (*WiCOM'08*), pp. 1-4, 2008. Article (CrossRef Link).
[25] B. Kar, P. P. Sahoo and A. K. Das, "A secure proxy blind signature scheme based on DLP," in *Proc. of International Conference on Multimedia Information Networking and Security* (*MINES*), pp. 477–480, 2010. Article (CrossRef Link).
[26] S. Pradhan and R. K. Mohapatra, "Proxy blind signature scheme based on ECDLP," *International Journal of Engineering Science & Technology*, vol. 3, no. 3, pp. 2244-2248, 2011.
[27] D. M. Alghazzawi, T. M. Salim and S. H. Hasan, "A new proxy blind signature scheme based on ECDLP," *International Journal of Computer Science Issues*, vol. 8, no. 1, pp. 73-79, 2011.

[28] C. H. Wang and M. Z. Liao, "Security analysis and enhanced construction on ECDLP-based proxy blind signature scheme," *International Journal of e-Education, e-Business, e-Management and e-Learning*, vol. 4, no. 1, pp. 47-51, 2014. Article (CrossRef Link).
[29] A. Sadat, I. Ullah, H. Khattak, S. Ullah and A. U. Rehman, "Proxy blind signcryption based on elliptic curve," *International Journal of Computer Science and Information Security*, vol. 14, no. 3, pp. 257-262, 2016.
[30] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)," *Lecture Notes in Computer Science*, Springer, vol. 1294, pp. 165-179, 1997. Article (CrossRef Link).
[31] H. M. Elkamchouchi, E. F. A. Elkhair and Y. Abouelseoud, "An efficient proxy signcryption scheme based on the discrete logarithm problem," *International Journal of Information Technology, Modeling and Computing*, vol. 1, no. 2, pp. 7-19, 2013. Article (CrossRef Link).
[32] R. Ullah, N. Uddin, A. I. Umar and N. Amin, "Blind signcryption scheme based on elliptic curves," in *Proc. of 2014 Conference on Information Assurance and Cyber Security (CIACS)*, IEEE Xplore Digital Library, pp. 51-54, 2014. Article (CrossRef Link).
[33] Shamsherullah, Nizamudin, A. I. Umar, Noorulamin, R. Ullah and I. Ullah, "Blind signcryption scheme based on hyper elliptic curve for untraceable payment system," in *Proc. of the 13th International Conference on Statistical Sciences*, Peshawar, Pakistan, vol. 28, pp. 337-344, 2015.
[34] C. X. Zhou, "Identity based generalized proxy signcryption scheme," *Information Technology and Control*, vol. 45, no. 1, pp. 13-26, 2016. Article (CrossRef Link).
[35] C. H. Lin, R. H. Hsu and L. Harn, "Improved DSA variant for batch verification." *Applied Mathematics and Computation*, vol. 169, no. 1, pp. 75-81, 2005. Article (CrossRef Link).
[36] C. F. Chou, W. C. Cheng and L. Golubchik, "Performance study of online batch-based digital signature schemes." *Journal of Network and Computer Applications*, vol. 33, no. 2, pp. 98-114, 2010. Article (CrossRef Link).
[37] C. H. Tsai and P. C. Su, "ECC-based multi-document fail-stop signature encryption scheme," *Journal of Internet Technology*, vol. 16, no. 3, pp. 461-473, 2015. Article (CrossRef Link).
[38] C. H. Tsai and P. C. Su, "Multi-document threshold signcryption scheme," *Security and Communication Network*, vol. 8, no. 13, pp. 2244-2256, 2015. Article (CrossRef Link).
[39] C. H. Tsai and P. C. Su, "An ECC-based blind signcryption scheme for multiple digital documents," *Security and Communication Networks*, vol. 2017, pp. 1-14, 2017. Article (CrossRef Link).
[40] V. S. Miller, "Use of elliptic curves in cryptography," *Lecture Notes in Computer Science*, Springer-Verlag, vol. 218, pp. 417-426, 1986. Article (CrossRef Link).
[41] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987. Article (CrossRef Link).
[42] V. B. Kute, P. R. Paradhi and G. R. Bamnote, "A software comparison of RSA & ECC," *International Journal of Computer Science and Applications*, vol. 2, no. 1, pp. 61-65, 2009.
[43] R. Sinha, H. K. Srivastava and S. Gupta, "Performance based comparison study of RSA and elliptic curve cryptography," *International Journal of Scientific & Engineering Research*, vol. 4, no. 5, pp. 720-725, 2013.
[44] A. J. Menezes and S. A. Vanstone, "Elliptic curve cryptosystems and their implementation," *Journal of Cryptology*, vol. 6, no. 4, pp. 209-224, 1993. Article (CrossRef Link).
[45] A. K. Lenstra and E. R. Verheul, "Selecting cryptographic key sizes," *Journal of Cryptology*, vol. 14, no. 4, pp. 255-293, 2001. Article (CrossRef Link).
[46] S. Gajbhiye, S. Karmakar, M. Sharma, S. Sharma and M. K. Kowar, "Application of elliptic curve method in cryptography: a literature review," *International Journal of Computer Science and Information Technologies*, vol. 3, no. 3, pp. 4499-4503, 2012.
[47] A. K. Tripathy, I. Patra and D. Jena, "Proxy blind signature based on ECDLP," *International Journal of Computer and Network Security*, vol. 2, no. 6, pp. 1-7, 2010.
[48] R. C. Wang, W. S. Juang and C. L. Lei1, "A web metering scheme for fair advertisement transactions," *International Journal of Security and Its Applications*, vol. 2, no. 4, pp. 49-56, 2008.

[49] N. Tahat, "A new signing algorithm based on elliptic curve discrete logarithms and quadratic residue problems," *Italian Journal of Pure and Applied Mathematics*, vol. 32, pp. 125-132, 2014.

Dr. Pin-Chang Su is presently working as an associate professor in the Department of Information Management at National Defense University, Taiwan. He received his Ph.D. degree in Electrical Engineering from Chang Gung University, Taiwan in 2007. His research mainly focuses on Algorithms Design in Error-Control Coding, Information Security, Cryptographic Systems and E-Commerce Technologies. His published articles can be found in most academic journals like Security and Communication Networks, Computers and Electrical Engineering, Journal of Internet Technology, Journal of Chung Cheng Institute of Technology and so forth.

Dr. Chien-Hua Tsai is currently an Associate Professor in the Department of Accounting Information at Chihlee University of Technology, Taiwan. He received his Ph.D. degree in Electrical Engineering and Computer Science from Case Western Reserve University, Ohio, USA in 2000. His research interests include Information System Security, Secure Communication Protocols, Public Key Cryptosystems and Electronic Transaction Security in Computer and Network Security. He has published several articles in most academic journals from Security and Communication Networks, Computers and Electrical Engineering, Journal of Internet Technology, Journal of e-Business and so on.