Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 7779152, 7 pages
https://doi.org/10.1155/2022/7779152

Research Article

An Efficient Multidocument Blind Signcryption Scheme for Smart Grid-Enabled Industrial Internet of Things

Ako Muhammad Abdullah,[1] **Insaf Ullah**,[2] **Muhammad Asghar Khan**,[2] **Mohammed H. Alsharif**,[3] **Samih M. Mostafa**,[4] **and Jimmy Ming-Tai Wu**[5]

[1]*University of Sulaimani, College of Basic Education, Computer Science Department, Sulaimaniyah, Kurdistan Region, Iraq*
[2]*Hamdard Institute of Engineering & Technology, Islamabad 44000, Pakistan*
[3]*Department of Electrical Engineering, College of Electronics and Information Engineering, Sejong University, Seoul 05006, Republic of Korea*
[4]*Faculty of Computers and Information, South Valley University, Qena 83523, Egypt*
[5]*College of Computer Science and Technology, Shandong University of Science and Technology, Shandong, China*

Correspondence should be addressed to Jimmy Ming-Tai Wu; wmt@wmt35.idv.tw

Received 29 November 2021; Accepted 5 January 2022; Published 21 February 2022

Academic Editor: Shalli Rani

The smart grid-enabled industrial Internet of Things (SG-IIoT) is a hybrid data communication network connected with the power grid that collects and analyzes data from transmission lines, distribution substations, and consumers. In the IIoT setting, SG provides predictive information to its supplier and customers on how to effectively manage the power based on this aggregated data. To achieve this goal, every virtual or physical entity in the SG-IIoT must be linked and accessible over the Internet, which can be susceptible to numerous cyberattacks. In this paper, we propose a multidocument blind signcryption scheme to simultaneously resolve the security and efficiency issues. The proposed scheme performs the blind signature and encryption operation on multiple digital documents in one step because SG-IIoT outputs a large amount of data that needs to be blind signed and encrypted in a batch. The proposed scheme employs the concept of hyperelliptic curve cryptography (HECC), which is lightweight owing to the smaller key size. The comparative analysis in both security and efficiency with the relevant existing scheme authenticates the viability of the proposed scheme.

1. Introduction

The electrical network that serves every residence, company, and infrastructure service in a city is known as the "grid." The "smart grid" is the next generation of energy infrastructure that has been upgraded with communications technology and connectivity to enable more efficient utilization of resources [1]. Wireless equipment such as sensors, radio modules, gateways, and routers are among the technologies that make today's IoT-enabled electricity grid "smart." These devices provide the advanced connection and communications that enable customers to make smarter energy consumption decisions, communities to save energy and money, and power authorities to restore power more rapidly after a blackout. Similar to distributed energy resources, real-time smart meter readings, rapid reaction through reliable communication and information exchange, and monitoring systems, it can manage the responsibilities of various applications across industrial processes [2]. The industrial Internet of Things (IIoT), also known as SG-enabled industrial Internet of Things, is growing popularity, and it includes a variety of IoT devices and technology that make smart grid (SG) for Industry 4.0 simpler [3], also known as SG-enabled industrial Internet of Things (SG-IIoT). The SG-IIoT infrastructure is built on faster and more reliable communication technologies that connect intelligent information systems,

the current power grid, and other IIoT devices. Furthermore, because industry 4.0 gadgets consume so much electricity, smart meters linked to them may need to request energy from power stations via substations and control centers (CC) [4]. Therefore, every virtual or physical thing in SG-IIoT can be interconnected, identified, and accessed through the Internet [5]. When evaluating the communication scenario of the SG-IIoT environment, authentication, confidentiality, and anonymity are the three key cybersecurity issues [6]. It is important to highlight that digital signatures can ensure authenticity, and anonymous encryption can ensure both confidentiality and anonymity. Blind signcryption [7] allows the sender to combine the concepts of blind signing and encryption on a message in a single step, achieving authenticity, confidentiality, and anonymity in one step. Further, making a blind signature and encryption on multiple digital documents is better than signcrypting a single document because SG-IIoT generates a huge amount of data that need to be blindly signcrypted in a bunch [8]. Most of the blindly signcryption, which is presented either for a single document or multi-digital documents is built upon the working strategy of old public key infrastructure (PKC) that can be poor in the view of the certificate renewal process. In contrast to PKC, identity-based cryptography (IBC) will be the best choice when the private key generation center is fully trusted, and further, IBC can enjoy the feature of certificate renewing and revocation-free features. Recently, several blind signcryptions are contributed to multi-digital documents; unfortunately, these schemes are not suitable for resource-hungry SG-IIoT devices due to higher computational cost and certificate renewing and revocation [8–10]. Thus, to neglect such types of flaws, we design a new scheme with the following advantages.

(i) The proposed scheme is based on the notion of blind signcryption with IBC for multi-digital documents utilizing hyperelliptic curve concepts for power requests in SG-IIoT

(ii) The proposed scheme ensures the integrity of multi-digital documents, nonrepudiation of blind signature, unlinkability of the signer to the multi-digital documents, untraceability of the signer to an original signature, confidentiality, and forward secrecy, respectively

(iii) When comparing the proposed scheme to three recently published relevant schemes, we observed that our scheme is more efficient in terms of computation and communication costs.

This paper is organized in the following way. In Section 2, we present the related work of existing blind signcryption and multidocument blind signcryption. In Section 3, we provide the proposed network model for power requests. Section 4 presents the construction of the proposed scheme. In Section 5, correctness is provided. Sections 6 and 7 provide security analysis and costs analysis in terms of computational cost, respectively. Lastly, in Section 8, conclusions are presented.

2. Related Work

The SG-IIoT configuration relies entirely on faster and more reliable communication technologies to connect intelligent information systems, existing power grids, and other IIoT devices. Every device in the SG-IIoT can be networked, identified, and connected to the Internet in this manner. Thus, during communications, the three key concerns of the SG-IIoT environment are anonymity, privacy, and validation. It is critical to understand that signatures can provide authentication and anonymity, while encryption can provide confidentiality to SG-IIoT data. Awasthi and Lal [7] devised a blind signcryption employing a discrete logarithm problem to meet authentication, confidentiality, and anonymity requirements in one step. This scheme does not provide forward secrecy and has a longer processing time as a result. Using the discrete logarithm problem, Xiuying and Dake [11] proposed a blind signcryption with public verifiability. More processing time is a problem for this scheme once again. Riaz et al. [12] developed an elliptic curve discrete logarithm problem for blind signcryption. Unforgeability, authentication, integrity, and signer nonrepudiation are all vulnerabilities in the scheme [13]. Furthermore, the authors in [13] presented an improved blind signcryption scheme, although when considering resource-hungry devices, this scheme suffers from higher processing CPU time owing to the elliptic curve. Mohib et al. [14] proposed an elliptic curve-based blind signcryption to allow anonymous communication to mobile voting systems. Waheed et al. [15] presented blind signcryption utilizing the elliptic curve discrete logarithm problem for the use of electronic voting. However, both schemes [14, 15] suffer from increased processing CPU time and are hence unsuitable for resource-intensive devices. Ullah and Din [16] presented blind signcryption using a hyperelliptic curve discrete logarithm problem; however, the approach does not ensure that numerous digital documents are encrypted and signed. Tsai et al. [8] suggested multidocument blind signcryption based on elliptic curve cryptography to offer encryption and blind signing in one step. They did not, however, provide forward security and did not benefit from the reduced computational cost. Blind signcryption using a hyperelliptic curve discrete logarithm issue was presented by Fazlullah et al. [9]. However, in terms of authentication and integrity, this technique is weak [10]. Furthermore, the authors of [10] suggested an enhanced multidocument blind signcryption system; nevertheless, when considering resource-hungry devices, this scheme suffers from increased processing CPU time needs due to more main operations of the hyperelliptic curve. Although, because they are all built on ancient public key infrastructure cryptography, all of the aforementioned blind signcryption techniques are prone to certificate revocation and renewal issues.

3. Network Model

Figure 1 depicts the flow of our proposed blind signcryption for multiple digital documents' scheme, which includes entities such as the industrial Internet of Things (IIoT), smart meters (SMs), substation (SS), private key generator (PKG),

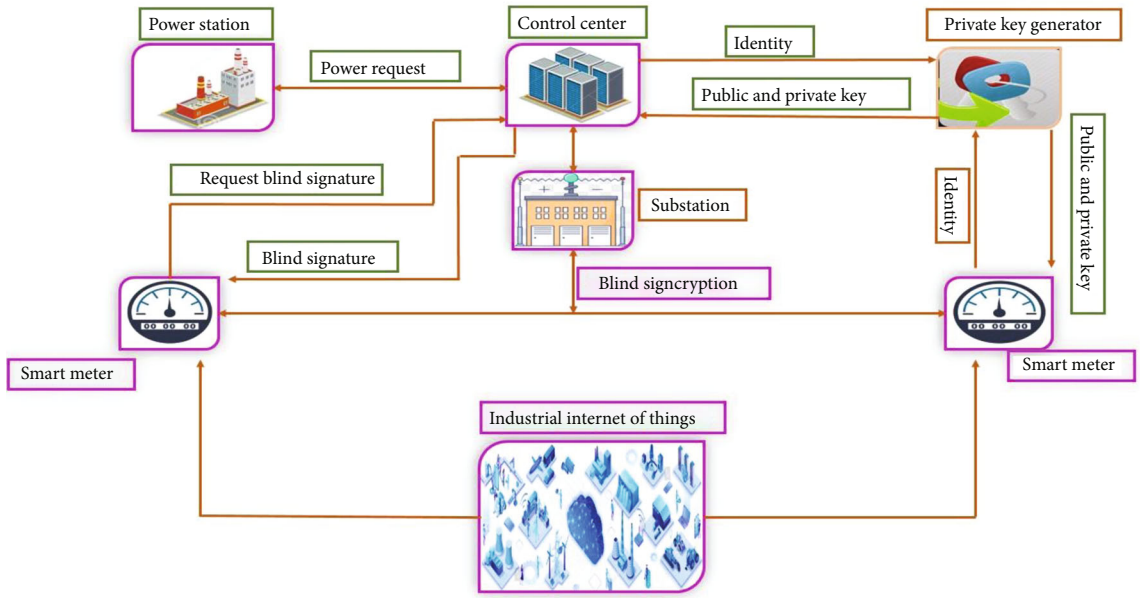

Figure 1: Network model of proposed SG-IIoT power request scheme [4].

Table 1: Symbols used in the constructions of the proposed algorithm.

No.	Symbol	Descriptions
1	H_1, H_2, H_3	One-way hash functions
2	ℓ	The private key of PKG
3	$\mathscr{D}$	Divisor of a hyperelliptic curve
4	n	The order of finite field of a hyper elliptic curve and normally greater or equals 80 bits
5	η	The public key of PKG
6	$\mathbb{A}$	Published parameter set
7	m_i	Multi-digital documents
8	U_s	Signer private key
9	V_s	Signer public key
10	U_v	Verifier private key
11	V_v	Verifier public key
12	φ	Alice signature
13	$\mathcal{S}$	Signer signature
14	K	The secret key used for encryption and decryption

and power station (PS). When IIoT requires more power or some other utility, SMs seek a blind signature from CC, after which CC sends its identity to PKG for a private and public key, and PKG generates a public and private key for CC after receiving the CC identity. After that, CC generates a blind signature for SMs using his private key and returns it. When SMs obtain a blind signature, they transmit their identification to PKG for a private and public key. When PKG receives the SMs' identity, it generates a public and private key for them. After that, SMs produce and submit blind signcryption on many papers, including power requests and other utilities to CC, using his private numbers and secret key. After receiving blind signcryption on numerous papers, CC can verify them using the verification method, then decode the ciphertext and supply power or other desired utilities to SMs if they are legitimate. Because all this information transmission is often in the range of a few bytes, LPWANs (low-power wide-area networks) are appropriate for interoperability of local micro-power grids. The low-power wide-area network (LPWAN) is a wide-area wireless communication network designed for long-range communications with low data rates and low power consumption.

4. Proposed Multidocument Blind Signcryption

The proposed multidocuments blind signcryption can continue with the following phases and the symbols used in construction is available in Table 1.

4.1. Setup. In private key generator (PKG), pick three one-way hash functions (H_1, H_2, H_3), hyperelliptic curve with genus 2, a divisor $(\mathscr{D})$, and a finite field of order n; then, PKG selects $\ell \in \{1, 2, 3, \cdots \cdots ., n-1\}$ as the private key of the signer and computes the corresponding master public key as $\eta = \ell.\mathscr{D}$. In the end, PKG published $\mathbb{A} = \{n, \mathscr{D}, H_1, H_2, H_3, \eta\}$ to the network

4.2. Key Generation. Here, PKG selects $U_i \in \{1, 2, 3, \cdots \cdots ., n-1\}$ as the private key and computes the corresponding public key as $V_i = U_i.G$ for the user with identity (ID_i). Then, PKG dispatched (U_i, V_i) to the user with ID_i using an open network

4.3. Alice. It can proceed with the following steps:

(a) Choose a random number $\ell \in \{1, 2, 3, \cdots \cdots ., n-1\}$

(b) Compute $V_h = H_1(\ell)$

Table 2: Major operations in proposed and existing schemes.

Schemes	Blind signcryption	Verifications and decryption	Total
Tsai et al. [8]	8 EM + 2 EA	4 EM	12 EM + 2 EA
Fazlullah et al. [9]	5 HEDM + 6 HEDA	3 HEDM + 2 HEDA	8 HEDM + 8 HEDA
Bashir and Ali [10]	8 HEDM + 6 HEDA	4 HEDM + 2 HEDA	12 HEDM + 8 HEDA
Proposed scheme	4 HEDM + 3 HEDA	3 HEDM + 3 HEDA	7 HEDM + 6 HEDA

Table 3: Computational cost comparison of proposed and existing scheme for a single message in milliseconds (ms).

Schemes	Blind signcryption	Verifications and decryption	Total
Tsai et al.[8]	$8 \times 2.226 + 2 \times 0.0288 = 17.8656$	$4 \times 2.226 = 8.904$	$12 \times 0.0288 + 2 \times 0.0288 = 26.7696$
Fazlullah et al. [9]	$5 \times 1.113 + 6 \times 0.0144 = 5.6514$	$3 \times 1.113 + 2 \times 0.0144 = 3.3678$	$8 \times 1.113 + 8 \times 0.0144 = 9.0192$
Bashir and Ali [10]	$8 \times 1.113 + 6 \times 0.0144 = 8.9904$	$4 \times 1.113 + 2 \times 0.0144 = 4.4808$	$12 \times 1.113 + 8 \times 0.0144 = 13.4712$
Proposed scheme	$4 \times 1.113 + 3 \times 0.0144 = 4.4952$	$3 \times 1.113 + 3 \times 0.0144 = 3.339$	$7 \times 1.113 + 6 \times 0.0144 = 7.8774$

Table 4: Computational cost comparison of proposed and existing scheme for a single message in milliseconds (ms).

Number of messages	Tsai et al. [8]	Fazlullah et al. [9]	Bashir and Ali [10]	Proposed scheme
50	1338.48	450.96	673.56	393.87
100	2676.96	901.92	1347.12	787.74
150	4015.44	1352.88	2020.68	1181.61

(c) Compute $\mathscr{R} = H_2(m_i, V_h)$

(d) Send $\mathscr{R}$ to the signer.

4.4. Signer. It can proceed with the following steps:

(a) Choose a random number $\mathscr{L} \epsilon \{1, 2, 3, \cdots \cdots ., n-1\}$

(b) Compute $T = \mathscr{L}.\mathscr{D}$

(c) Compute $\mathscr{S} = (U_s + \mathscr{R}.\mathscr{L}) \bmod n$

(d) Sends $(T, \mathscr{S})$to signer.

4.5. Alice. It can proceed with the following steps:

(a) Select random number $\zeta \epsilon \{1, 2, 3, \cdots \cdots ., n-1\}$

(b) Compute $Z = \zeta.\mathscr{D}$

(c) Choose a random number $\mathscr{T} \epsilon \{1, 2, 3, \cdots \cdots ., n-1\}$, compute $K = H_3(\mathscr{T}.V_v)$

(d) Compute $C = E_K(m_I, V_h)$

(e) Compute $\varphi = \mathscr{T}/(\zeta + \mathscr{R} + \mathscr{S}) \bmod n$

(f) Send $\mathfrak{A} = (\mathrm{C}, \mathrm{T}, \varphi, \mathrm{Z}, \mathscr{R})$.

4.6. Verifications and Decryption. It can proceed with the following steps:

(a) Compute $K = H_3(\varphi.U_v.(V_s + \mathscr{R}.(T + \mathscr{D}) + Z)$

(b) Compute $m_i, V_h = D_K(C)$

(c) Compute $P = H_2(m_i, V_h)$

(d) Accept if $P = \mathscr{R}$.

5. Correctness

The blind signcryption scheme can be correct if it holds the below equation.

$$H_3(\varphi.U_i.(V_s + \mathscr{R}.(T + \mathscr{D}) + Z) = \mathscr{T}.V_i. \quad (1)$$

Proof:

$$\begin{aligned}
&= H_3(\varphi.U_v.(U_s.\mathscr{D} + \mathscr{R}.(T + \mathscr{D}) + Z)) \\
&= H_3(\varphi.U_v.(U_s.\mathscr{D} + \mathscr{R}.(\mathscr{L}.\mathscr{D} + \mathscr{D}) + Z)) \\
&= H_3(\varphi.U_v.(U_s.\mathscr{D} + \mathscr{R}.\mathscr{L}.\mathscr{D} + \mathscr{R}.\mathscr{D} + \mathscr{K}.\mathscr{D})) \\
&= H_3\left(\frac{\mathscr{T}}{\zeta + \mathscr{R} + \mathscr{S}}.U_v.(U_s.\mathscr{D} + \mathscr{R}.\mathscr{L}.\mathscr{D} + \mathscr{R}.\mathscr{D} + \zeta.\mathscr{D})\right) \\
&= H_3\left(\frac{\mathscr{T}}{\zeta + \mathscr{R} + U_s + \mathscr{R}.\mathscr{L}}.U_v.(U_s + \mathscr{R}.\mathscr{L} + \mathscr{R} + \zeta)\mathscr{D}\right) \\
&= H_3(\mathscr{T}.U_v.\mathscr{D}) = H_4(\mathscr{T}.V_v) = K
\end{aligned} \quad (2)$$

6. Security Analysis

This phase includes detailed security analysis of the proposed scheme, which are based on the following hard problem: suppose $P\&\mathscr{D}$ is given two divisors on the hyperelliptic curve of order n: hence, to find a unique integer α from equation $P = \alpha.\mathscr{D}$ is called hyperelliptic curve discrete logarithm problem ($\mathscr{HECDLP}$). So, in the following subphases of this section, we are going to explain each security requirement fulfilled by the proposed scheme in detail.

6.1. Confidentiality. Suppose an adversary $\mathscr{A}$ attacked the proposed scheme for gaining the contents of ciphertext (C) ; then it must successfully be passed through the following subphases.

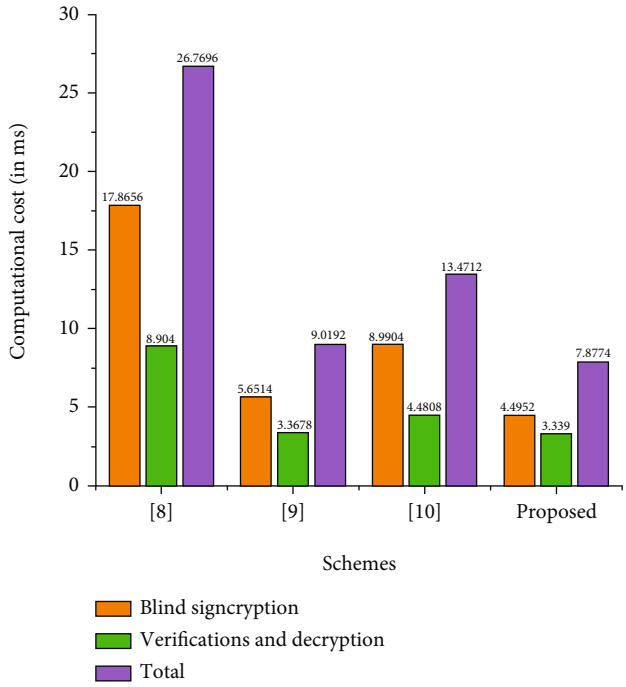

Figure 2: Computational cost comparisons for a single message.

(i) Here, the first attempt of $\mathscr{A}$ as it needs to process $K_s = H_3(\varphi.U_v.(V_s + \mathscr{R}.(T + \mathscr{D}) + Z)$ further requires U_v from $V_v = U_v.\mathscr{D}$ that can be clues towards the solution of $\mathscr{HECDLP}$

(ii) The second attempt of $\mathscr{A}$ needs to process $K_s = H_3(\mathscr{T}.V_v)$, so it requires $\mathscr{T}$ that can be clues towards the solution of $\mathscr{HECDLP}$

(iii) The third attempt of $\mathscr{A}$ needs $\mathscr{T}$ from $\varphi = \mathscr{T}/(\zeta + \mathscr{R} + \mathscr{S})$ to process $K_s = H_3(\mathscr{T}.V_v)$, so φ contains two unknown hyperelliptic curve variables which are infeasible for $\mathscr{A}$.

The above three subphases indicate that the proposed scheme is secured from the content-stealing attack (confidentiality) against $\mathscr{A}$.

6.2. Unforgeability. Assume that $\mathscr{A}$ attacked the proposed scheme for forging the original signature; then $\mathscr{A}$ must effectively solve $\varphi = \mathscr{T}/(\zeta + \mathscr{R} + \mathscr{S})$ for this; it passed through the following subphases.

(i) Here, the first thing is that $\mathscr{A}$ can require $\mathscr{T}$, and for this, $\mathscr{A}$ must process $K_s = H_3(\mathscr{T}.V_v)$, so it requires $\mathscr{T}$ that can be clues towards the solution of $\mathscr{HECDLP}$

(ii) The second thing is that $\mathscr{A}$ requires ζ, and for this, it process $Z = \zeta.\mathscr{D}$, so it requires ζ that can be clues towards the solution of $\mathscr{HECDLP}$

(iii) The third attempt of $\mathscr{A}$ needs $\mathscr{S}$ from $\varphi = \mathscr{T}/(\zeta + \mathscr{R} + \mathscr{S})$, where $\mathscr{S} = (U_s + \mathscr{R}.\mathscr{L}) \bmod n$, so $\mathscr{S}$ contains two unknown hyperelliptic curve variables which are infeasible for $\mathscr{A}$.

The above three subphases indicate that the proposed scheme is secured from forging attack (unforgeability) against $\mathscr{A}$.

6.3. Message Integrity. In our designed scheme, with ciphertext, the sender appends and computes $\mathscr{R} = H_2(m_i, V_h)$ as a hash value and is dispatched to the receiver. After the reception, the receiver can verify using the following steps.

(i) It computes the new hash value after decrypting the ciphertext as $P = H_2(m_i, V_h)$

(ii) Then compare $P = \mathscr{R}$, if it equals then accept the ciphertext; otherwise it returns a null value.

The above two steps indicate that the proposed scheme is secured from the content modifying attack (message integrity) against $\mathscr{A}$.

6.4. Blindness. In our designed scheme, when the signer acts as $\mathscr{A}$, then he just failed to get m_i, from $\mathscr{R} = H_2(m_i, V_h)$, because of the one-way nature of the hash function. Also, $\mathscr{A}$ requires to proceed first the blind factor $V_h = H_1(\ell)$, and for this, $\mathscr{A}$ needs ℓ which is the private number of Alice, so we can say that the proposed scheme is secure from unfair signer attack (blindness).

6.5. Untraceability. Suppose the signer acts as $\mathscr{A}$ when it received $\mathfrak{A} = (C, T, \varphi, Z, \mathscr{R})$ and tries to gain the contents of ciphertext (C), forging the original signature $\varphi = \mathscr{T}/(\zeta + \mathscr{R} + \mathscr{S}) \bmod n$. Therefore, for gaining the contents of the ciphertext (C),it must be successfully passed through the following subphases.

(i) Here, the first attempt of $\mathscr{A}$ needs to process $K_s = H_3(\varphi.U_v.(V_s + \mathscr{R}.(T + \mathscr{D}) + Z)$; further, it requires U_v from $V_v = U_v.\mathscr{D}$ that can be clues towards the solution of $\mathscr{HECDLP}$

(ii) The second attempt of $\mathscr{A}$ needs to process $K_s = H_3(\mathscr{T}.V_v)$, so it requires $\mathscr{T}$ that can be clues towards the solution of $\mathscr{HECDLP}$

(iii) The third attempt of $\mathscr{A}$ needs $\mathscr{T}$ from $\varphi = \mathscr{T}/(\zeta + \mathscr{R} + \mathscr{S})$ to process $K_s = H_3(\mathscr{T}.V_v)$, so φ contains two unknown hyperelliptic curve variables which are infeasible for $\mathscr{A}$.

The above three subphases indicate that the proposed scheme is secured from the signer to get access to the content of an original text.

Also, forging the original signature $\varphi = \mathscr{T}/(\zeta + \mathscr{R} + \mathscr{S}) \bmod n$, it must successfully be passed through the following subphases.

(i) Here, the first thing is that $\mathscr{A}$ can require $\mathscr{T}$, and for this, $\mathscr{A}$ must process $K_s = H_3(\mathscr{T}.V_v)$, so it requires $\mathscr{T}$ that can be clues towards the solution of $\mathscr{HECDLP}$

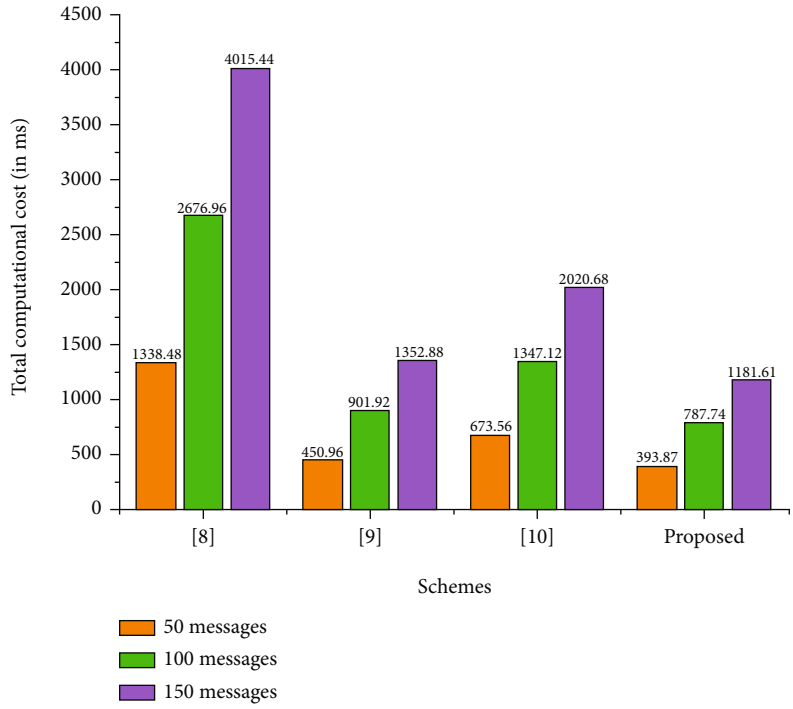

Figure 3: Computational cost comparisons for 50, 100, and 150 messages.

(ii) The second thing is that $\mathscr{A}$ requires ζ, and for this, it processes $Z = \zeta.\mathscr{D}$, so it requires ζ that can be clues towards the solution of $\mathscr{HECDLP}$.

The above two subphases indicate that the proposed scheme is secured from forging attacks against the signer. Further, the above discussion indicates that the proposed scheme is secured from an untraceable attack against the signer.

6.6. Forward Secrecy. The designed scheme assures the property of message forward secrecy. Suppose an adversary $\mathscr{A}$ attacked the proposed scheme for gaining the contents of ciphertext (C); then it must successfully be passed through the following subphases.

(i) The first attempt of $\mathscr{A}$ needs to process $K_s = H_3(\mathscr{T}.V_v)$, so it requires $\mathscr{T}$ that can be clues towards the solution of $\mathscr{HECDLP}$

(ii) The second attempt of $\mathscr{A}$ needs $\mathscr{T}$ from $\varphi = \mathscr{T}/(\zeta + \mathscr{R} + \mathscr{S})$ to process $K_s = H_3(\mathscr{T}.V_v)$, so φ contains two unknown hyperelliptic curve variables which are infeasible for $\mathscr{A}$.

The above three subphases indicate that if the private key signer or Alice is compromised, then the proposed scheme is still secured from the content-stealing attack (forward secrecy) against $\mathscr{A}$.

6.7. Authentication. Upon reception of $\mathfrak{A} = (C, T, \varphi, Z, \mathscr{R})$, the receiver can proceed with it compute $K = H_3(\varphi.U_v.(V_s + \mathscr{R}.(T + \mathscr{D}) + Z)$, $m_i, V_h = D_K(C)$, $P = H_2(m_i, V_h)$, and accept if $P = \mathscr{R}$. So, the authentication will be done in this way in our proposed scheme.

6.8. Nonrepudiation. The blinded signature $\mathscr{S} = (U_s + \mathscr{R}.\mathscr{L})$ mod n which is processed by the signer contains the signer's private key which is directly associated with its public key; that is why in our scheme, the signer cannot deny his generated signature.

7. Computational Cost

For the computational cost comparisons, we first introduce some notations that are EM, EA, HEDM, and HEDA representing elliptic curve point multiplication, elliptic curve point addition, hyperelliptic curve divisor multiplication, and hyperelliptic curve divisor addition. The experiment is done for the running time of a single EM and EA, with the help of a personal computer containing DUAL CPU E2200, 2.20 gigahertz processor, 2048 megabyte primary memory; EM consumes 2.226 ms and EA takes 0.0288 ms [17, 18]. Therefore, for HEDM and HEDA, we assume the half running time of EM and EA are 1.113 ms and 0.0144 ms, because the hyperelliptic curve consumes half of the elliptic curve [19]. The major operations proposed and those of Tsai et al. [8], Fazlullah et al. [9], and Bashir and Ali [10] are presented in Table 2. Then, based on the above major operations running time, in Tables 3 and 4, we present the running time comparison between the proposed scheme and Tsai et al. [8], Fazlullah et al. [9], and Bashir and Ali [10], for single message and a varying number of messages. In the end, Figures 2 and 3 clearly show that our scheme is efficient in requiring the processing time.

8. Conclusions

In this article, we proposed a multidocument blind signcryption scheme to concurrently address security concerns such as untraceability, confidentiality, and forward secrecy, as well as efficiency challenges such as high computation cost. Because SG-IIoT generates a considerable quantity of data that has to be blind signed and encrypted in a batch, the proposed scheme executes the blind signature and encryption operation on numerous digital documents in one step. The proposed scheme makes use of the hyperelliptic curve cryptography (HECC) idea, which is lightweight because of its lower key size. We performed a security analysis study for the proposed scheme, confirming our view that our scheme is more secure and capable of meeting data exchange security requirements such as untraceability, confidentiality, and forward secrecy. Furthermore, an efficiency study of the proposed scheme in terms of computational cost reveals that our scheme is more efficient than the relevant existing schemes.

Data Availability

All data generated or analyzed during this study are included in this published article.

Conflicts of Interest

The authors declare no conflict of interest.

Authors' Contributions

Conceptualization and supervision are by Ako Muhammad Abdullah and Muhammad Asghar Khan. Original draft writing and methodology are by Insaf Ullah. Formal analysis is by Mohammed H. Alsharif. Validation is by Samih M. Mostafa. Software is by Ako Muhammad Abdullah. Conceptualization and review and editing are by Jimmy Ming-Tai Wu.

References

[1] S. M. A. A. Abir, A. Anwar, J. Choi, and A. S. M. Kayes, "IoT-enabled smart energy grid: applications and challenges," *IEEE Access*, vol. 9, pp. 50961–50981, 2021.

[2] J. L. Gallardo, M. A. Ahmed, and N. Jara, "LoRa IoT-based architecture for advanced metering infrastructure in residential smart grid," *IEEE Access*, vol. 9, pp. 124295–124312, 2021.

[3] A. Ghasempour, "Internet of things in smart grid: architecture, applications, services, key technologies, and challenges," *Inventions*, vol. 4, no. 1, p. 22, 2019.

[4] W. Zhang, Z. Guo, N. Li, M. Li, Q. Fan, and M. Luo, "A blind signature-aided privacy-preserving power request scheme for smart grid," *Wireless Communications and Mobile Computing*, vol. 2021, Article ID 9988170, 10 pages, 2021.

[5] I. Ullah, N. Ul Amin, M. Zareei et al., "A lightweight and provable secured certificateless signcryption approach for crowd sourced IIoT applications," *Symmetry*, vol. 11, no. 11, p. 1386, 2019.

[6] M. Kaveh, S. Aghapour, D. Martin, and M. R. Mosavi, "A secure lightweight signcryption scheme for smart grid communications using reliable physically unclonable function," *2020 IEEE International Conference on Environment and Electrical Engineering and 2020 IEEE Industrial and Commercial Power Systems Europe*, 2020, pp. 1–6, Madrid, Spain, June 2020.

[7] A. K. Awasthi and S. Lal, "Efficient scheme for sensitive message transmission using blind signcryption," in *Proceedings of the International Conference on Communication*, Kumabakonam India, December 2004.

[8] C.-H. Tsai and P.-C. Su, "An ECC-based blind signcryption scheme for multiple digital documents," *Security and Communication Networks*, vol. 2017, Article ID 8981606, 14 pages, 2017.

[9] N. U. Fazlullah, J. Amin, A. Iqbal, I. Umar, and M. Shahid, "Secure and efficient protocol for transmission of multi digital documents using blind signcryption," *International Journal of Computer Science and Network Security*, vol. 18, no. 6, pp. 68–78, 2018.

[10] M. Z. U. Bashir and R. Ali, "Cryptanalysis and improvement of a blind multi-document signcryption scheme," *Cryptologia*, vol. 45, no. 5, pp. 450–464, 2021.

[11] Y. Xiuying and H. Dake, "A new efficient blind signcryption," *Wuhan University Journal of Natural Sciences*, vol. 13, no. 6, pp. 662–664, 2008.

[12] R. Ullah, A. I. Umar, and N. Ul Amin, "Blind signcryption scheme based on elliptic curves," *2014 Conference on Information Assurance and Cyber Security*, 2014, pp. 51–54, Rawalpindi, Pakistan, June 2014.

[13] M. Zia and R. Ali, "Cryptanalysis and improvement of blind signcryption scheme based on elliptic curve," *Electronics Letters*, vol. 55, no. 8, pp. 457–459, 2019.

[14] A. Waheed, N. Din, A. I. Umar, R. Ullah, and N. -u. Amin, "Novel blind signcryption scheme for E-voting system based on elliptic curves," *Mehran University Research Journal of Engineering and Technology*, vol. 40, no. 2, pp. 314–322, 2021.

[15] M. Ullah, A. I. U. Nizamuddin, N. Amin, and S. Amin, "An efficient mobile phone voting system based on blind signcryption," in *4th International Conference on Computer and Emerging Technologies*, Shah Abdul Latif University, Khairpur Mirs, Pakistan, March 2014.

[16] S. Ullah and N. Din, "Blind signcryption scheme based on hyper elliptic curves cryptosystem," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 917–932, 2021.

[17] H. H. Kilinc and T. Yanik, "A survey of SIP authentication and key agreement schemes," *Ieee Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1005–1023, 2014.

[18] S. A. Chaudhry, H. Alhakami, A. Baz, and F. Al-Turjman, "Securing demand response management: a certificate-based access control in smart grid edge computing infrastructure," *IEEE Access*, vol. 8, pp. 101235–101243, 2020.

[19] M. A. Khan, I. Ullah, A. Alkhalifah et al., "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 5, 2020.