Hindawi
Mobile Information Systems
Volume 2020, Article ID 4138516, 13 pages
https://doi.org/10.1155/2020/4138516

*Research Article*

# Certificateless Proxy Reencryption Scheme (CPRES) Based on Hyperelliptic Curve for Access Control in Content-Centric Network (CCN)

**Zahid Ullah,[1] Asim Zeb,[2] Insaf Ullah,[3] Khalid Mahmood Awan,[4] Yousaf Saeed,[5] M. Irfan Uddin,[6] Mahmoud Ahmad Al-Khasawneh,[7] Marwan Mahmoud,[8] and Mahdi Zareei[9]**

[1]*Department of Physical and Numerical Sciences, Qurtuba University of Science and Information Technology, Peshawar Campus, 25000 KP, Pakistan*
[2]*Department of Computer Science, Abbottabad University of Science and Technology, 22500 Havelian, KP, Pakistan*
[3]*HIET, Hamdard University Karachi, Islamabad Campus, 44000 Islamabad, Pakistan*
[4]*Department of Computer Science, COMSATS University Islamabad, Attock Campus, Attock, Pakistan*
[5]*Department of Information Technology, University of Haripur, 22620 Haripur, Pakistan*
[6]*Institute of Computing, Kohat University of Science and Technology, 26000 Kohat, KP, Pakistan*
[7]*Faculty of Computer & Information Technology, Al-Madinah International University, Kuala Lumpur, Malaysia*
[8]*King Abdulaziz University, Jeddah, Saudi Arabia*
[9]*Tecnologico de Monterrey, School of Engineering and Sciences, Zapopan 45201, Mexico*

Correspondence should be addressed to Asim Zeb; asimzeb1@gmail.com

Received 26 January 2020; Revised 23 May 2020; Accepted 10 June 2020; Published 25 July 2020

Academic Editor: Sungchang Lee



Information-centric networking is the developing model envisioned by an increasing body of the data communication research community, which shifts the current network paradigm from host centric to data centric, well-known to information-centric networking (ICN). Further, the ICN adopts different types of architectures to extend the growth of the Internet infrastructure, e.g., name-based routing and in-network caching. As a result, the data can be easily routed and accessed within the network. However, when the producer generates contents for authentic consumers, then it is necessary for him/her to have a technique for content confidentiality, privacy, and access control. To provide the previously mentioned services, this paper presents a certificateless proxy reencryption scheme (CPRES) based on the hyperelliptic curve for access control in the content-centric network (CCN). Using certificateless PRE, the power of the key generation center (KGC) is limited to only the generation of partial keys to secure the access to the content. With the help of these partial keys, the producer further calculates keys for encryption and reencryption process. The simulation results show that the proposed scheme provides secure access to content during end-to-end communication. Moreover, the proposed CPRES scheme outperforms in terms of low computational energy and efficient utilization of communication bandwidth.

## 1. Introduction

Information-centric networking (ICN) is an approach to develop the Internet infrastructure to directly support the unique named data [1]. The ICN attracts much attention in the continuing search for a future communication model of the Internet [2]. It shifts the networking model from the current host-centric model, where all requests for content are made to a host identified by its Internet protocol (IP) address(es), to the data-centric model [3]. Table 1 depicts the differences among both the networks, i.e., host centric and ICN [4]. An ICN named content can be stored anywhere in the network, and each content object can be uniquely addressed and requested.

Content-centric networking (CCN) is the most encouraging architecture of ICN paradigms, which performs

Table 1: Host centric vs ICN.

| | Host centric | ICN |
|---|---|---|
| Routing | Using IP addresses | Name-based routing |
| Caching | Specific caching points | Each node can cache the content |
| Security | Communication channels | Secure the content |
| API | Data send to a specific address | Publish and subscribe contents |

communication by using two specialized kinds of packets, i.e., interest packet and data packet, which carry a name to uniquely identify the requested content [5]. The interest packet is used to advertise a user's request to obtain the interested data, as shown in Figure 1, while the data packet is used to return the corresponded content to the user [6]. Compared with the host-based conversation model of current IP architectures, the content delivery in ICN follows a receiver pushed back method. Once the requested content is matched in ICN, the data are transferred to the receivers with the reverse method.

Therefore, the objective of ICN is to find, publish, and distribute network contents rather than the reachability of end hosts and keep host-to-host discussions between them [6]. For more clarifications, the system model of ICN is shown in Figure 2, where it includes four basic parties [3, 7], namely, content producers; secondly, routers; thirdly, edge service router; and lastly, content consumers. Here, the content producer is responsible for generating the content, converting data to named data objects with desired security bindings and protections, and publishing it in the network.

The routers are responsible to forward requests for data objects and also provide a platform for communication between the consumers and the producer. Routers are composed of three primary elements: (i) forwarding information base (FIB), (ii) pending interest table (PIT), and (iii) content store (CS) [3]. The FIB is used to route incoming interests to the appropriate output port towards the desired content producer. Much like traditional IP routing tables, the FIB is populated using standard routing protocols or static routes and matches content names in interest packets to FIB entries using the longest prefix match. The PIT serves as a cache of the interest state such that content objects that satisfy interests may follow the reverse interest path back to the requester. This preserves upstream and downstream network flow. Finally, the CS is an optional cache for content objects that, if present, is first searched prior to forwarding an interest upstream. These caches serve to reduce content object retrieval latency and bandwidth consumption in the network.

The edge service routers placed at the edge of the ICN network domain have the additional features that allow publishers to deploy certain services such as processing data, forwarding encrypted data to the proper destination, and also storing the content [7]. Lastly, the content consumer downloads the encrypted content from the edge service router through their interest and decrypts with the help of the desired decryption key.

As the Internet shifts from IP-based communication to a content name-based approach, this model will face some critical challenges, for example, mobility, security, access control, routing, naming, and caching [8].

By keeping in view the above observations, access control is one of the most significant techniques for authentication and

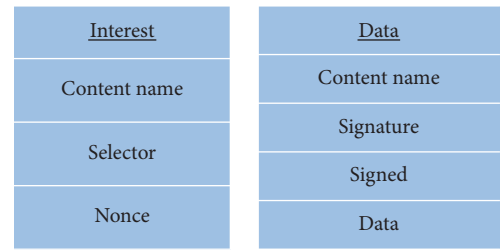


Figure 1: (a) Interest packet and (b) data packet.

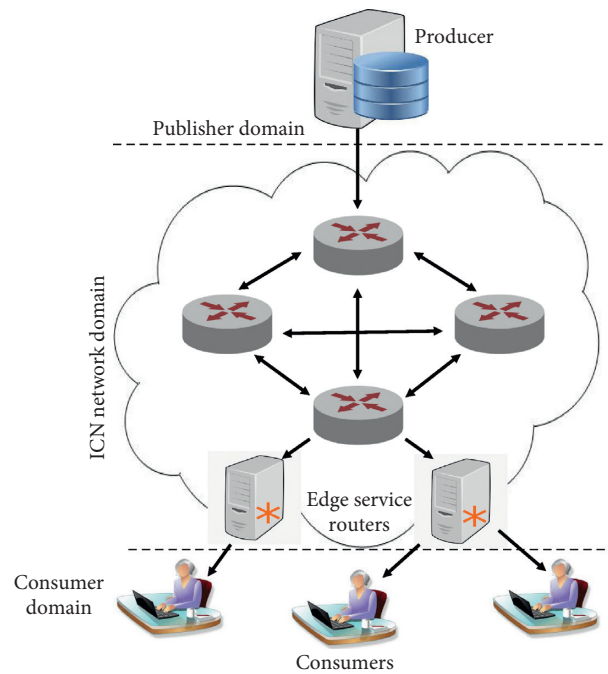


Figure 2: ICN system model.

accessing of contents of the ICN architecture. As contents are retrieved from distributed in-network caches, there should be a security mechanism, which ensures the contents' protection and users' authorizations [9]. Since a number of proposals are available in the literature, which can be fruitful for access control, but to the best of our investigation, the certificateless proxy reencryption is the most prominent and securable scheme. So, a certificateless proxy reencryption scheme is the best choice for improving the efficiency and security level because it generates the partial secret key to reduce the extra efforts of the key generation center (KGC) and control the misuse of the secret key.

Motivated by the above insight, the certificateless proxy reencryption scheme based on the hyperelliptic curve for access control is a newly recommended scheme for CCN in this paper. The certificateless proxy reencryption eliminates the key escrow problem that is found in the identity-based proxy reencryption scheme (IB-PRE) [10]. According to our investigatory study, the security hardiness and efficiency of existing IB-PRE and certificateless proxy reencryption are based on the standard cryptosystems like Rivest, Shamir, and Adleman (RSA), elliptic curve (EC), and bilinear pairing (BP). The RSA uses a 1024-bit key and public and private parameter sizes, while EC uses 160 bits, where BP is 13.65 ms worse than RSA and 13.93 ms worse than the elliptic curve according to the experimental results in [11], and also 14.42 ms worse than the hyperelliptic curve from the assumption in [12]. The proposed scheme hyperelliptic curve uses 80 bits for the parameter size providing the same level of security along with low computational and communication cost.

*1.1. Motivations and Contributions.* To provide a better and secure networking structure to the information-centric network, the researchers are interested to put more efforts in this field to push the research forward. In this sequence, recently, Wood [10] proposed an identity-based proxy reencryption (IB-PRE) scheme based on elliptic curve cryptography for CCN. But, any proper mechanism for security analysis and algorithm was not specified. Also, the key escrow problem ambiguity was indicated in the IB-PRE scheme. Furthermore, in a recent research in 2019, Wang et al. [13] proposed another PRE scheme using BP cryptography based on the random oracle model. So, the current trends among the cryptographic researchers are that they believe on practical analysis instead of theoretical, e.g., the random oracle model. Furthermore, besides from these two schemes, which are specific to the ICN, a number of public key infrastructure (PKI), identity based, and certificateless signature methods are available in the literature for providing applications to different communication systems [13–17]. The computational and communication cost of this crypto system is so much higher because of using the known cryptographic protocol parameters and key sizes, i.e., RSA uses 1024 bits, where BP is almost 13.65 times worse than RSA, 13.93 times than EC, and 14.42 than the hyperelliptic curve [12], respectively. So, to continue the same debate, by using the results in [12], the EC is 0.28 times faster than RSA and the hyperelliptic curve is 0.48 times faster than EC and 0.77 times quicker than RSA.

As concluded from the above discussion, we found that there is no such scheme, which has formal security analysis and is not suffering from extra computational and communication cost. So, the motivation of our research is to propose a unique CPRES scheme to solve the above-mentioned problems in the form of the certificateless proxy reencryption scheme based on the hyperelliptic curve for access control in content-centric networking. Our contribution is listed in the following steps.

(i) We proposed a certificateless proxy reencryption scheme based on the hyperelliptic curve for access control in content-centric networking.

(ii) Our scheme utilizes an 80-bit key instead of the bilinear pairing and the elliptic curve which use 1024-bit key and 160-bit key, respectively.

(iii) Our scheme removes the key escrow problem of identity-based PRE by using CL-PRE.

(iv) In terms of computational and communication cost, our scheme is more efficient as compared to the models proposed in [7, 8, 18, 19] and other existing schemes [13, 17, 20–25].

(v) We provide our security analysis through a recognized security validation tool known as AVISPA.

## 2. Related Work

*2.1. Access Control.* Access control (AC) is the main selected area of the proposed scheme. A number of schemes are proposed for AC in CCN to provide accessibility to only authorized users. The researchers divide an access control method into two ways: namely, encryption-based access control and encryption independent [26]. The encryption-based access control mechanism is further categorized into four ways, i.e., broad encryption, PKI-based encryption, attribute-based encryption, and identity-based encryption. Furthermore, the PKI-based encryption is implemented in three ways, i.e., session based, proxy reencryption, and probabilistic model. This article relates to the proxy reencryption mechanism; so, here, we focus on proxy reencryption access control mechanisms.

The reencryption process is performed by an intermediate proxy node for each consumer; Wood et al. [18] proposed a flexible scheme using the combination of identity-based encryption and proxy reencryption for secure communication. Before the content distribution, the producer encrypts the content with a symmetric key. The consumer can retrieve content from either the producer or the cache node. After receiving the encrypted content by the consumer, it requests a symmetric key from the producer, and the producer verifies the consumer validity and access level and then sends the encrypted symmetric key using the consumer identity to a verifier consumer. The consumer uses this key for decryption of the content.

Another context for AC is proposed by Mangili et al. [19]. In this context, the content is divided into partitions and then fragments. Further, the producer performed two-level encryptions: firstly, the fragments are encrypted using a symmetric key into a chunk, and this chunk is stored in an encrypted form; secondly, the encryption is performed for collusion elimination and confidentiality which uses the "key regression" method for generation of the key chain based on the key derivation algorithm [27]. Using a secure encrypted access obtained from the producer, the authorized consumer regenerates the second-level encryption key. The producer reencrypts the encrypted chunks only for the authorized consumer to protect the collusion.

A unique AC framework was proposed by Zheng et al. [7] for ICN. In this framework, the encryption process is performed by the edge routers. Firstly, the publisher encrypts the content with the public key and k1 as a random key. When the

consumer sends a request for content access, the edge router selects k2 as a random key and performs the reencryption on encrypted content. The edge router uses the publisher's public key to encrypt the random key k2, attaches it with the content, and then sends it to the consumer. Before the decryption, the consumer sends their identity, content, name, and k2 to the publisher for verification. The publisher generates another key $k$, after the verification of the consumer access level and identity using the private key, along with k1 and k2 for the consumer. The consumer decrypts the content using key $k$. The decryption key $k$ is different for every consumer due to the generation of key k2 randomness of each request.

*2.2. Certificateless Proxy Reencryption (CL-PRE).* For the first time, Blaze et al. [28] presented the concept of PRE in 1998. It was, however, bidirectional and colluding insecure. Following Blaze et al.'s PRE scheme, Ateniese et al. [29] improved it in the form of a unidirectional PRE scheme based on paillier encryption. Later, they proposed two more schemes: chosen plaintext attack (CPA) secure schemes based on the bulletin board system with pairing and two-level encryption schemes. The first chosen ciphertext attack (CCA) was improved by Canneti and Hohenberger [30] in the form of the secure bidirectional multihop PRE scheme. Further, this work was extended by Libert and Vergnaud [31] to make it the chosen ciphertext attack (CCA2) scheme in order to make it more secure and to make reencrypted ciphertext publicly verifiable. First, the CCA2 secure pairing-free bidirectional PRE scheme based on ElGamal encryption and Schnorr's signature was proposed by Deng et al. in [32]. They made it efficient than previous paradigms and left the possibility for the construction of a CCA2 secure PRE scheme in a standard model. It was ultimately solved by Wang et al. in [33] using Cramer–Shoup encryption [34]. They compared their efficiency with the work of Canneti and Hohenberger [30].

To solve the certification management problem in PRE, Green and Ateniese [14] proposed employed conventional PRE in an identity-based (IB) setup, for the first time in 2007. Many other unidirectional IB-PRE schemes have been proposed [35, 36] in the same year. However, the schemes in [35, 37] are insecure against the collusion attack in which a private key of the delegator can be extracted by proxy. Later, Wang et al. proposed in [15] another IB-PRE scheme based on the random oracle model, and Mizuno and Doi [38] designed one more IB-PRE algorithm based on the chosen plaintext attack security using a standard model. Using the standard model, another CCA-secure IB-PRE scheme was proposed by Shao and Cao in [39]. The first CCA-secure single-hop IB-PRE based on the standard model to maintain conditional reencryption was introduced by Liang et al. in [40]. Further, in 2014, Liang et al. continued their work and designed a cloud-based revocable IB-PRE scheme in which ciphertexts are reencrypted by proxy under an identity and time period in [41]. However, Wang et al. proved in [36] that Liang's scheme in [40] is weak against collusion and reencryption key dummy attack although the withdrawal users decrypt the encrypted data after time expires which was allowed by it. They further proposed the improved version using the standard model based on expensive pairing operations.

Another ambiguity is exposed in identity-based encryption in the form of the key escrow problem. It provides growth, for instance, to certificateless PRE (CL-PRE). CL-PRE developed with pairing for the first time was presented by Sur et al. in [42], and since then, this development has attracted more attention from academia and research community. They claimed their scheme to be CCA-secure, but Zheng et al. proved in [43] that the concrete attack is possible in their scheme. CL-PRE scheme for data distributing with the public cloud using encryption-based access control and key management was designed by Xu et al. [20] in 2012. They claimed its security against a chosen plaintext attack. To increase the security and efficiency level, they further designed the multiproxy and randomized CL-PRE scheme. In 2013, replayable CCA-secure PRE scheme based on the random oracle model was proposed by Guo et al. [23] to verify that Xu et al.'s scheme in [20] is weak against type I adversary. The above schemes [20,23,42] were based on expensive bilinear pairing operations. To conclude the PRE literature, only few pairing-free CL-PRE schemes exist. The first pairing-free CL-PRE scheme was proposed by Lee and Han [24] in 2014. Also, they compared their work with Xu et al.'s [20] and Sur et al.'s [42] schemes and proved that their scheme is better in terms of confidentiality and computation time. In 2014, to improve the security models in [24], a CCA-secure bidirectional CL-PRE scheme was proposed by Wang et al. [16]. However, for reencryption process, proxy has required secret keys of both the sender and the receiver.

Qin et al. [25] proposed another CL-PRE scheme in 2015 for data distributing in cloud and compared its security with CCA based on the strong security model. However, any formal security analysis was not provided by them. The simulation results proved that their scheme performance is better than Xu et al.'s scheme [20], Sur et al.'s scheme [42], and Lee and Han's scheme [24] in terms of storage and communication overhead.

Another CCA-secure unidirectional and single-hop CL-PRE scheme was proposed by Srinivasan and Rangan [22]. They broke the confidentiality of the scheme in [24] and proved that it is insecure. They also compared their work in terms of efficiency with Guo et al.'s scheme [23]. The proposed scheme of Srinivasan and Rangan [22] required several precalculations to perform the key generation process. It could also be stored locally. As a result, it increased the storage capacity, which was not suitable for constrained resource devices.

Recently, in 2018, Bhatia et al. [17] proposed another CL-PRE scheme for health care environment based on elliptic curve cryptography which uses a 160-bit key size. They compared their scheme efficiency with the schemes in [20, 22–25, 42] in terms of computational and communication cost. Furthermore, in a recent research in 2019, the PRE scheme for access control in ICN was proposed by Qiang Wang et al. [13] which is based on the random oracle model using bilinear pairing cryptography.

## 3. Materials and Methods

*3.1. Preliminaries.* First time in 1988, Koblitz designed the EC simplification form to upholding class of the curve, known as hyperelliptic curve (HEC). The HEC performance is more remarkable when compared to that of the elliptic

curve (EC), and it uses a smaller key with the same security level [44]. To break the HEC security is more difficult due to the solution of the hyperelliptic curve discrete logarithm problem (HECDLP) [45]. Also, HEC provides more suitable environment for resource-constrained devices.

Let us suppose $\mathscr{CRV}$ is the curve on the field $\digamma n$ and $\digamma n$ is the finite set on this field in order $n$. The length of the type one curve on the field $\digamma n$ is as long as "$n$" $\log 2\, n \approx 2^{160}$. Also, the length of the type two curve on the field $\digamma n$ with $|\digamma n| \approx 2^{80}$ is 80 bits [44, 45].

Let the finite field of HEC be $\digamma$, the algebraic closure be $\bar{\digamma}$ over the field $\digamma$, and $\mathscr{CRV} > 1$ be the type of curve of HEC on $\digamma$. The solution set is described as $(\mathscr{I}, j) \in \digamma * \digamma$. Equation (1) represents the HEC which is as follows:

$$\mathscr{CRV}:\ j2 + h(\mathscr{I})j = f(\mathscr{I}). \tag{1}$$

So, $h(\mathscr{I}) \in \digamma[\mathscr{I}]$ and $f(\mathscr{I}) \in \digamma[\mathscr{I}]$ are polynominal of degree $\mathscr{G}$ and monic polynomial of degree $2\mathscr{G} + 1$, respectively. To calculate equation (1), there is no solution set of $(\mathscr{I}) \in \bar{\digamma} * \bar{\digamma}$. Hyperelliptic curve at $\mathscr{G} = 1$ is the specific case of the elliptic curve [44].

Furthermore, the hyperelliptic curve discrete logarithm problem (HECDLP) is populated by its own in the field of cryptography because of providing the hard security level. It is used in different cryptographic approaches, e.g., ElGamal [46], based on the discrete logarithm problem.

The HECDLP is defined as suppose $D$ is the divisor from $\mathscr{CRV}$ and $\ell$ is the integer which belongs to $\digamma n$, so finding $\ell$ from $y = \ell.D$ is said to be HECDLP.

*3.2. Architecture of Proposed Model.* The proposed certificateless proxy reencryption scheme for AC in CCN is described in Figure 3, which contains four basic parties, i.e., key generation center (KGC), producer, edge service router, and consumer, respectively. Firstly, the producer and the consumer send their identity (IDpr and IDcr) to the KGC. The KGC calculates the master public key $\mathscr{L} = \delta.\mathscr{L}$ and publishes the parameters $\psi = \{HEC, Fn, n, n \le 280, \mathscr{L}, L, h\}$. Further, the KGC delivers the partial private key $\mathscr{G}\mathrm{p} = (\alpha\mathrm{p}, \beta\mathrm{p})$ using the secure network and the partial public key $\mathscr{Q}\mathrm{p} = (\mathscr{X}\mathrm{p}, \mathscr{Y}\mathrm{p}, \mathscr{Z}\mathrm{p}, \gamma\mathrm{p})$ using the insecure network to each participant with their identity IDp, and then each participant, using their identity IDp, sets a secret value $\mathscr{U}\mathrm{p} = (\mathscr{J}\mathrm{p}, \mathscr{H}\mathrm{p})$ and generates private and public keys $\mathscr{P}\mathrm{p} = (\alpha\mathrm{p}, \beta\mathrm{p}, \mathscr{J}\mathrm{p}, \mathscr{H}\mathrm{p})$ and $\mathscr{PB}\mathrm{p} = (\mathscr{X}\mathrm{p}, \mathscr{Y}\mathrm{p}, \mathscr{Z}\mathrm{p}, \gamma\mathrm{p}, \mathscr{B}\mathrm{p}, \mathscr{I}\mathrm{p})$. Also, the producer generates a reencryption key $\Omega$ for level-2 encryption. In this process, it takes the input, identity IDpr, public and private keys ($\mathscr{P}$pr and $\mathscr{PB}$pr) of the producer, public key of the consumer $\mathscr{PB}$cr, and the identity of the consumer IDcr. Now, the level-1 encryption is performed by the producer on the content (CNT) by taking input the public key $\mathscr{PB}$pr of the producer and public parameters $\psi$ and this encrypted content is sent along with the reencryption (level-2) key $\Omega$ to the concerned edge service router using a secure channel. Further, the edge service router performed reencryption (level-2) process using the reencryption key $\Omega$ and public parameters $\psi$, and also computes $\mathscr{C}1^* = \mathscr{C}1 \oplus \Omega$ and $\mathscr{C}2^* = \mathscr{C}2$ and

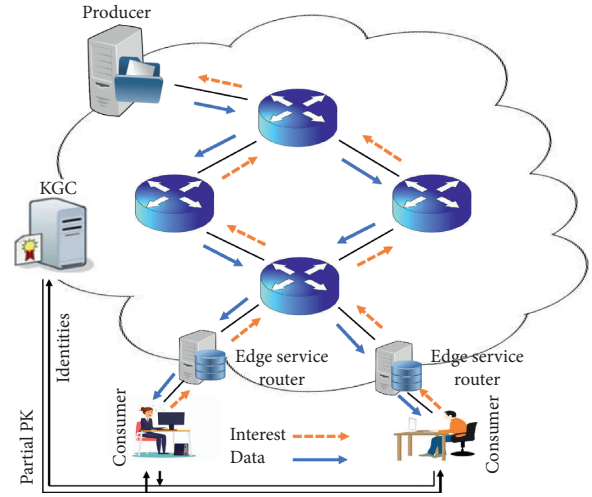


Figure 3: Architecture of the proposed CL-PRE scheme for access control in CCN.

sends the pair $\Phi = (\mathscr{C}1^*, \mathscr{C}2^*)$ to the consumer. Finally, the consumer takes input $\Phi = (\mathscr{C}1^*, \mathscr{C}2^*)$ and $(\mathscr{G}\mathrm{cr}, \mathscr{J}\mathrm{cr}, \mathscr{H}\mathrm{cr})$ to decrypt the content.

*3.3. Basic Notation.* Table 2 represents the basic notations that are used in the proposed algorithm.

## 4. Construction of Proposed Algorithm

The proposed certificateless proxy reencryption scheme CPRES algorithm includes the following nine phases:

*Setup.* In this phase, the KGC selects a security $\Upsilon$ and hyperelliptic curve (HEC) over the field $Fn$ of order $n \le 280$, suppose $\mathscr{L}$ is the divisor on HEC of order $n$. Further, KGC picks a secret key $\delta \in \{1,2, \ldots\ldots, n\text{-}1\}$ and calculates a master public key as $L = \delta.\mathscr{L}$. Finally, the parameters $\psi = \{HEC, Fn, n, n \le 280, \mathscr{L}, L, h\}$ are published.

*Partial Private Key Extract (PPKE).* In this PPKE phase, the KGC first randomly selects three numbers $x, y, z \in \{1, 2, \ldots, n-1\}$ and calculates $\mathscr{X}\mathrm{p} = x.\mathscr{L}$, $\mathscr{Y}\mathrm{p} = y.\mathscr{L}$, and $\mathscr{Z}\mathrm{p} = z.\mathscr{L}$. It further computes $\alpha\mathrm{p} = x + \delta\,(\mathrm{IDp}, \mathscr{X}\mathrm{p})$, $\beta\mathrm{p} = y + \delta.(\mathrm{IDp}, \mathscr{Y}\mathrm{p})$, and $\gamma\mathrm{p} = z + \delta.(\mathrm{IDp}, \mathscr{Z}\mathrm{p}, \mathscr{X}\mathrm{p}, \mathscr{Y}\mathrm{p})$. Then, KGC delivers a partial private key $\mathscr{G}\mathrm{p} = (\alpha\mathrm{p}, \beta\mathrm{p})$ utilizing the secure network and the partial public key $\mathscr{Q}\mathrm{p} = (\mathscr{X}\mathrm{p}, \mathscr{Y}\mathrm{p}, \mathscr{Z}\mathrm{p}, \gamma\mathrm{p})$ utilizing the insecure network, to each participant with identity IDp.

*Set Secret Value (SSV).* In SSV, each participant with identity IDp selects two random numbers $\mathscr{J}\mathrm{p}$ and $\mathscr{H}\mathrm{p} \in \{1,2, \ldots\ldots, n\text{-}1\}$, as a secret value $\mathscr{U}\mathrm{p} = (\mathscr{J}\mathrm{p}, \mathscr{H}\mathrm{p})$.

*Generate Private Key (GPK).* In GPK, each participant with identity IDp generates the private key $\mathscr{P}\mathrm{p} = (\alpha\mathrm{p}, \beta\mathrm{p}, \mathscr{J}\mathrm{p}, \mathscr{H}\mathrm{p})$. In this process, it takes input the partial private key $\mathscr{G}\mathrm{p}$ and secret value $\mathscr{U}\mathrm{p}$.

*Generate Public Key (GPBK).* In GPBK, each participant with identity IDp first computes $\mathscr{B}\mathrm{p} = \mathscr{J}\mathrm{p}.\mathscr{L}$ and $\mathscr{I}\mathrm{p} = \mathscr{H}\mathrm{p}.\mathscr{L}$ and generates the public key $\mathscr{PB}\mathrm{p} = (\mathscr{X}\mathrm{p}, \mathscr{Y}\mathrm{p},$

Table 2: Notations of the proposed scheme.

| S.no | Notation | Description |
|---|---|---|
| 1 | HEC | Hyper elliptic curve from the finite field $Fn$ having order $n$ |
| 2 | $n$ | It is a large prime number, and the order is $n \leq 280$ |
| 3 | $\psi$ | Public parameter set |
| 4 | $\Upsilon$ | Symbolizes the input security parameter from the hyperelliptic curve |
| 5 | $\delta$ | Master secret key of KGC |
| 6 | $\mathscr{L}$ | Master public key of KGC |
| 7 | $h$ | Irreversible or one-way hash function |
| 8 | $\mathscr{L}$ | Divisor on HEC |
| 9 | $\mathscr{G}$pr, $\mathscr{G}$cr | Partial private keys for producer and consumer |
| 10 | $\mathscr{Q}$pr, $\mathscr{Q}$cr | Partial public keys for producer and consumer |
| 11 | $\mathscr{J}$pr, $\mathscr{H}$pr | Secret values of producer |
| 12 | $\mathscr{J}$cr, $\mathscr{H}$cr | Secret values of consumer |
| 13 | $\mathscr{P}$pr, $\mathscr{P}$cr | Full private keys of producer and consumer |
| 14 | $\mathscr{PB}$pr, $\mathscr{PB}$cr | Public keys of producer and consumer |
| 15 | IDpr, IDcr | Identities of producer and consumer |
| 16 | $\Omega$ | Reencryption key |
| 17 | CNT | It means the contents (plain text) |
| 18 | $Lfk$ | Level-1 encryption key |
| 19 | $Lfk^*$ | Level-2 decryption key |
| 20 | Npr | Fresh nonce |
| 21 | $\mathscr{C}$pr | Level-1 encryption |
| 22 | $\Phi$ | Level-2 encryption |
| 23 | $\oplus$ | Used for encryption and decryption |

$\mathscr{X}$p, $\gamma$p, $\mathscr{B}$p, $\mathscr{J}$p). In this process, it takes input the partial public key $\mathscr{Q}$p and secret value $\mathscr{U}$p.

*Generate Reencrypt Key (GREK).* in GREK, the producer generates a proxy reencryption key $\Omega$ for level-2 encryption. In this process, it takes input the identity of the producer IDpr, the public and private keys ($\mathscr{P}$prand $\mathscr{PB}$pr), the public key of the consumer $\mathscr{PB}$cr, and the identity of the consumer IDcr. The following steps more clearly explain the generation of the proxy reencryption key:

Compute $Q\text{pr} = \mathscr{X}\text{cr} + L$ (IDcr, $\mathscr{X}$cr)

Compute $Q\text{pr} = (\mathscr{J}\text{pr}, Q\text{pr}, \alpha\text{pr}. \mathscr{J}\text{cr}, \text{IDpr}, \text{IDcr}, \mathscr{PB}\text{pr}, \mathscr{PB}\text{cr})$

Compute $\Omega = ((\alpha\text{pr} + \mathscr{J}\text{pr}) (\mathscr{X}\text{pr}, \mathscr{Y}\text{pr}, \mathscr{B}\text{pr}, \mathscr{J}\text{pr}) + \alpha\text{pr} + \mathscr{H}\text{pr}) Q\text{pr}$

*Level-1 Encrypt.* In this L-1 phase, the producer generates the level-1 encryption on content (CNT), by taking input the public key $\mathscr{PB}$pr of the producer and public parameters $\psi$. The following are the steps:

Choose nonce Npr

Choose $\mathscr{O} \in \{1,2, \ldots\ldots..,n\text{-}1\}$

Compute $\mathscr{R} = h$ (CNT, Npr, $\mathscr{B}$pr, IDpr, $\mathscr{I}$ pr)

Compute $\mathscr{C}1 = \mathscr{R}.\mathscr{L}$, compute $\mathscr{C}3 = \mathscr{O}.\mathscr{L}$

Compute level-1 encryption key $Lfk = (\mathscr{R}$ $((\mathscr{X}\text{pr} + (\text{IDpr}, \mathscr{X}\text{pr}) + \mathscr{B}\text{pr})$ $(\mathscr{X}\text{pr}, \mathscr{Y}\text{pr}, \mathscr{B}\text{pr}, \mathscr{I}\text{pr}) + \mathscr{Y}\text{pr} + \mathscr{L}$ $(\text{IDpr}, \mathscr{Y}\text{pr}) + \mathscr{I}\text{pr}))$

Compute $\mathscr{C}2 = (\text{CNT}, \text{Npr}) \oplus Lfk$

Compute $\mathscr{C}4 = \mathscr{O} + (\mathscr{C}1, \mathscr{C}2, \mathscr{C}3)$ and return $\mathscr{C}\text{pr} = (\mathscr{C}1, \mathscr{C}2, \mathscr{C}3, \mathscr{C}4)$ for proxy

*Level-2 (Reencrypt).* In this L-2 phase, the edge serves router generates the level-2 encryption on level-1 cipher text, by taking input the reencryption key $\Omega$ and public parameters $\psi$. The edge service router first computes $\mathscr{C}1^* = \mathscr{C}1 \oplus \Omega$ and $\mathscr{C}2^* = \mathscr{C}2$ and sends the pair $\Phi = (\mathscr{C}1^*, \mathscr{C}2^*)$ to the consumer.

*Decryption.* This process takes input $\Phi = (\mathscr{C}1^*, \mathscr{C}2^*)$ and ($\mathscr{G}$cr, cr, $\mathscr{H}$cr) and produces the plaintext. The consumer performs the following steps:

Compute $Q\text{cr} = \mathscr{X}\text{pr} + L$ (IDpr, $\mathscr{X}$pr)

Compute $Q\text{cr} = (\mathscr{B}\text{pr}. \alpha\text{cr}, Q\text{cr}. \mathscr{H}\text{cr}, \text{IDpr}, \text{IDcr}, \mathscr{PB}\text{pr}, \mathscr{PB}\text{cr})$

Compute $Lfk^* = (\mathscr{C}1^*)/Q\text{cr}$

Decrypt $(\text{CNT}, \text{Npr}) = \mathscr{C}2^* \oplus Lfk^*$

## 5. Security Analysis

Detailed analysis of the proposed scheme with respect to showing the resistance against the intruders included confidentiality (level-1 and level-2) and replay attack which are given below.

*5.1. Confidentiality of Level-1 Encryption.* Confidentiality is a rule to block the access of an unauthorized user to the secure and protected data. So, in this proposed scheme, when the intruders want to get the actual content, they must have a level-1 encryption secret key, that is, $Lfk$, and $Lfk = (\mathscr{R}$ $((\mathscr{X}\text{pr} + (\text{IDpr}, \mathscr{X}\text{pr}) + \mathscr{B}\text{pr})$ $(\mathscr{X}\text{pr}, \mathscr{Y}\text{pr}, \mathscr{B}\text{pr}, \mathscr{I}$ pr) + $\mathscr{Y}\text{pr} + \mathscr{L}$ $(\text{IDpr}, \mathscr{Y}\text{pr}) + \mathscr{I}\text{pr}))$. It is very hard for intruders to find $Lfk$ because in $Lfk$, the producer concatenates

Table 3: Computational cost comparisons on the basis of major operations.

| Schemes | Involves participants | | | | |
|---|---|---|---|---|---|
| | Reencryption | Encryption | Proxy reencryption | Decryption | Total |
| Xu et al.'s [20] | 2 EXPO | 3 EXPO + 1 BPR | 3 EXPO + 1 BPR | 2 BPR | 8 EXPO + 4 BPR |
| Guo et al.'s [23] | 5 EXPO | 3 EXPO + 2 BPR | 5 EXPO + 1 BPR | 8 EXPO + 2 BPR | 21 EXPO + 5 BPR |
| Lee and Han's 1 [24] | 3 EXPO | 4 EXPO | 1 EXPO | 4 EXPO | 12 EXPO |
| Lee and Han's 2 [24] | 3 EXPO | 5 EXPO | 3 EXPO | 10 EXPO | 21 EXPO |
| Wang et al.'s [25] | 3 EXPO | 4 EXPO | 1 EXPO | 7 EXPO | 15 EXPO |
| Srinivasan and Rangan's [22] | 5 EXPO | 8 EXPO | 1 EXPO | 6 EXPO | 20 EXPO |
| Bhatia et al.'s [17] | 4 PM | 5 PM | 1 PM | 7 PM | 17PM |
| Wang et al.'s [13] | 1 EXPO | 2 SM + 2 BPR | 1 BPR | 1 BPR + 1 SM | 1 EXPO + 3 SM + 4 BPR |
| Proposed | 4 HDM | 5 HDM | 1 HDM | 3 HDM | 13 HDM |

his/her own private key, i.e., $\mathcal{I}$p, with other parameters. Further, the intruder calculates $\mathcal{I}$p from $\mathcal{I}\text{p} = \mathcal{H}\text{p}$ which is harder due to the hyperelliptic curve discrete logarithm problem (HECDLP).

*5.2. Confidentiality of Level-2 Encryption.* In this phase, the confidentiality of the proposed scheme is analyzed for both cases for intruders and also for the key generation center (KGC), i.e., the part of the network.

*Case 1.* Again, when the intruders want to get the content, they must have a level-2 encryption (reencryption) secret key, that is, $\Omega$, and $\Omega = ((\alpha\text{pr} + \mathcal{J}\text{pr})\ (\mathcal{X}\text{pr}, \mathcal{Y}\text{pr}, \mathcal{B}\text{pr}, \mathcal{I}\text{pr}) + \alpha\text{pr} + \mathcal{H}\text{pr})$ Qpc. Due to the use of the producer partial private key $\alpha$pr and $\alpha\text{p} = x + \delta$ (IDp, $\mathcal{X}$p) it is very hard for intruders to calculate the level-2 encryption secret key.

*Case 2.* Also, for KGC they must need $\mathcal{B}$pr and $\mathcal{B}\text{pr} = \mathcal{J}\text{p}.\mathcal{L}$. To find $\mathcal{B}$pr again, they must calculate hyperelliptic curve discrete logarithm problem (HECDLP) that is infeasible for KGC.

*5.3. Replay Attack.* In our proposed algorithm, the producer generates and associates a nonce (Npr) value with every content like (CNT, Npr). This nonce value is the identity of every content. If any active intruder tries to send messages regularly for disturbance or breaking the communication, the producer can easily identify due to this nonce identity value. So, our proposed scheme is fully safe from replay attack.

## 6. Performance Evaluation

We evaluate our proposed approach in terms of different properties, e.g., computational and communication overhead, in Tables 3 and 4 and Figures 4 and 5, respectively.

*6.1. Computational Cost.* The comparison of the proposed scheme in terms of the computational cost with the latest contribution to the certificateless proxy reencryption scheme, i.e., Xu et al. [20], Guo et al. [23], Lee and Han [24], Wang et al. [25], Srinivasan and Rangan [22], Bhatia et al. [17], and Wang et al. [13], is illustrated. To show this, we select the major operations, for example, bilinear pairing operation (BPR), modular exponential (EXPO), elliptic curve point multiplication (PM), and hyperelliptic curve divisor multiplication (HDM), in the proposed scheme and those by Xu et al. [20], Guo et al. [23], Lee and Han [24], Wang et al. [25], Srinivasan and Rangan [22], Bhatia et al. [17], and Wang et al. [13] for computational cost comparisons. Further, the cost of the abovementioned major operations is shown in Table 3, with respect to proposed and the existing schemes. Also, the computational cost comparison is calculated with respect to milliseconds (ms), illustrated in Table 4. To demonstrate the computational time in milliseconds of different cryptographic operations, we use the theoretical results of schemes [12, 47] such as a single BPR consumes 14.90 ms, EXPO consumes 1.25 ms, scalar multiplication on $G$ takes 4.31 ms, PM consumes 0.97 ms, and HDM consumes 0.48 ms, respectively. As a result, the proposed scheme reduces the computational cost up to 91.26% from the recent research scheme [13], and the differentiation from other schemes is shown in Figure 4.

Further, a recognized formula ((existing framework-–proposed method) divided by (existing framework)) to calculate the reduction of the computational cost in millisecond is used, see [12]. Now, the difference of the proposed scheme's computational cost from other schemes is as follows: difference from Xu et al.'s scheme [20] is (8 EXPO + 4 BPR − 13 HDM)/(8 EXPO + 4 BPR) = (69.6 − 6.24)/69.6 ∗ 100 = 91.03%, from Guo et al.'s scheme [23] is (21 EXPO + 5 BPR − 13 HDM)/(21 EXPO + 5 BPR) = (100.75 − 6.24)/100.75 ∗ 100 = 93.806 vvv%, from Lee and Han's scheme 1 [24] is (12 EXPO − 13 HDM)/(12 EXPO) = (15–6.24)/15 ∗ 100 = 58.4%, from Lee and Han's scheme 2 [24] is (21 EXPO − 13 HDM)/(21 EXPO) = (26.25 − 6.24)/26.25 ∗ 100 = 76.22%, from Wang et al.'s scheme [25] is (15 EXPO − 13 HDM)/(15 EXPO) = (18.75 − 6.24)/18.75 ∗ 100 = 66.72%, from Srinivasan and Rangan's scheme [22] is (20 EXPO − 13 HDM)/(20 EXPO) = (25–6.24)/25 ∗ 100 = 75.04%, from Bhatia et al.'s scheme [17] is (17 PM − 13 HDM)/(17 PM) = (16.49 − 6.24)/16.49 ∗ 100 = 62.15%, and from Wang et al.'s scheme [13] is (1 EXPO + 3 SM + 4 BPR − 13 HDM)/(1 EXPO + 3 SM + 4 BPR) = (73.78 − 6.24)/73.78 ∗ 100 = 91.54%, respectively. In Figure 5, we illustrate the difference of computational cost of the proposed scheme from that of Xu et al.'s [20], Guo et al.'s [23], Lee and Han's 1 [24],

Table 4: Computational cost comparisons on the basis of millisecond.

| Schemes | Involves participants | | | | |
|---|---|---|---|---|---|
| | Reencryption (ms) | Encryption (ms) | Proxy reencryption (ms) | Decryption (ms) | Total (ms) |
| Xu et al.'s [20] | 2.5 | 18.65 | 18.65 | 29.08 | 69.6 |
| Guo et al.'s [23] | 6.25 | 33.55 | 21.15 | 39.8 | 100.75 |
| Lee and Han's 1 [24] | 3.75 | 5 | 1.25 | 5 | 15 |
| Lee and Han's 2 [24] | 3.75 | 6.25 | 3.75 | 12.5 | 26.25 |
| Wang et al.'s [25] | 3.75 | 5 | 1.25 | 8.75 | 18.75 |
| Srinivasan and Rangan's [22] | 6.25 | 10 | 1.25 | 7.5 | 25 |
| Bhatia et al.'s [17] | 3.88 | 4.85 | 0.97 | 6.79 | 16.49 |
| Wang et al.'s [13] | 1.25 | 38.42 | 14.90 | 19.21 | 73.78 |
| Proposed | 1.92 | 2.4 | 0.48 | 1.44 | 6.24 |

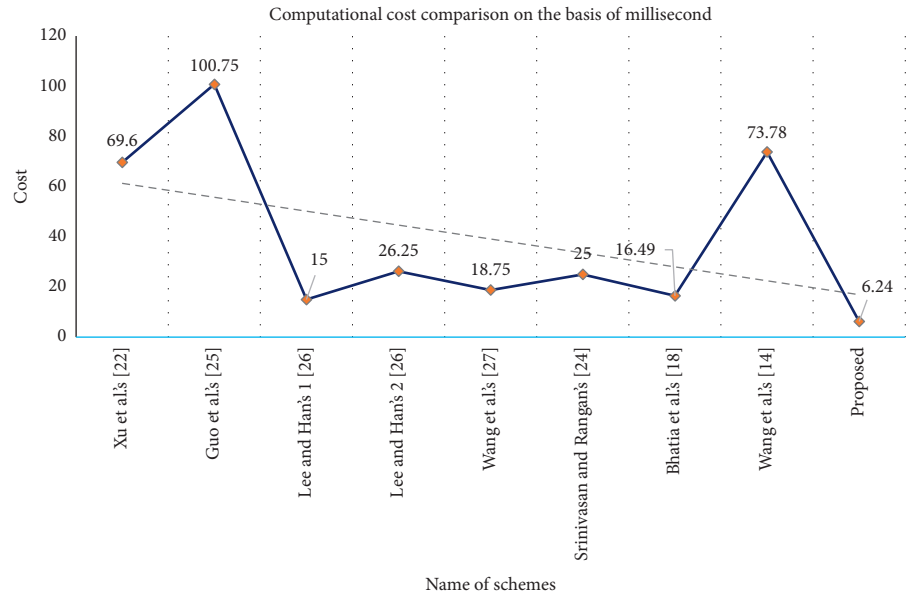


Figure 4: Computational cost comparison in millisecond.

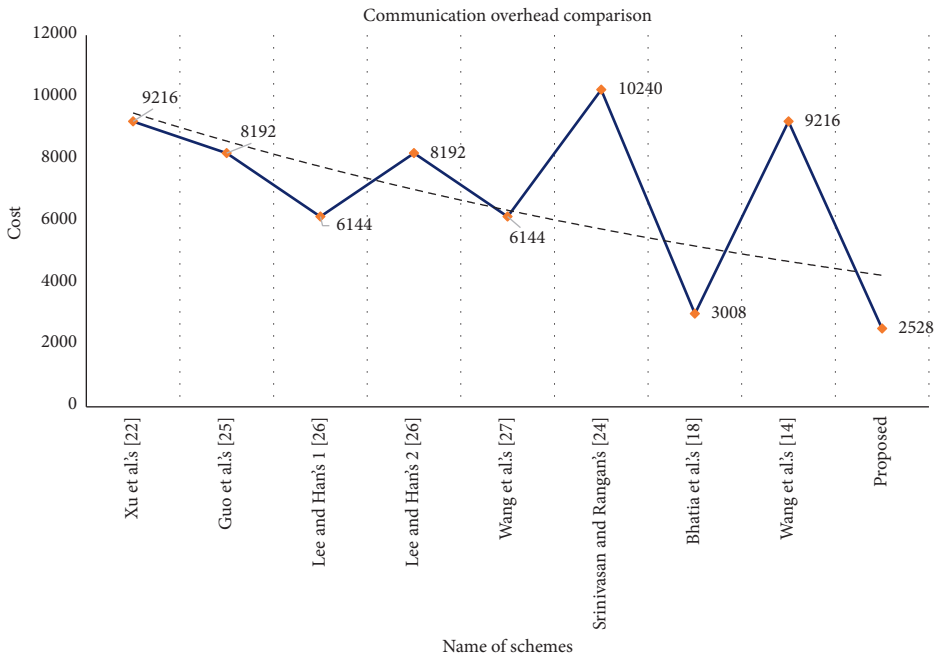


Figure 5: Communication overhead comparison.

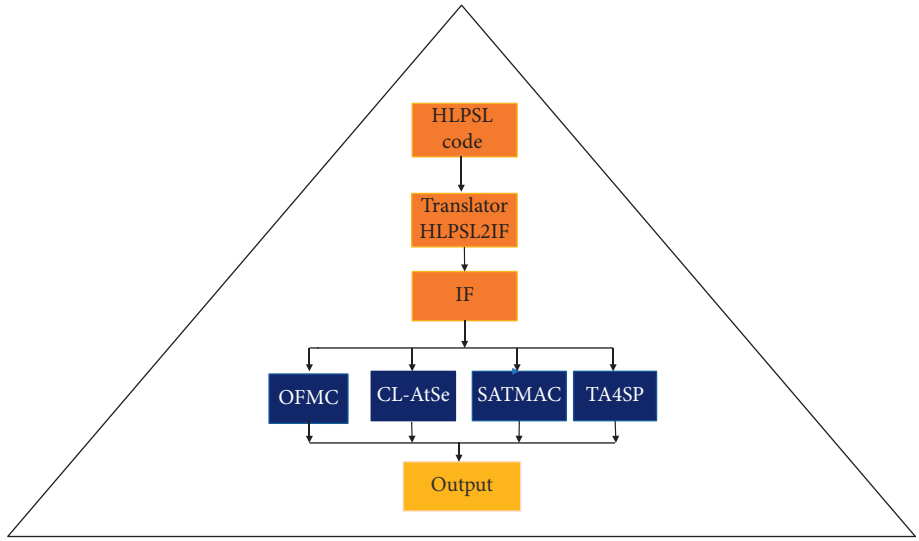


Figure 6: Basic architecture of the AVISPA tool.

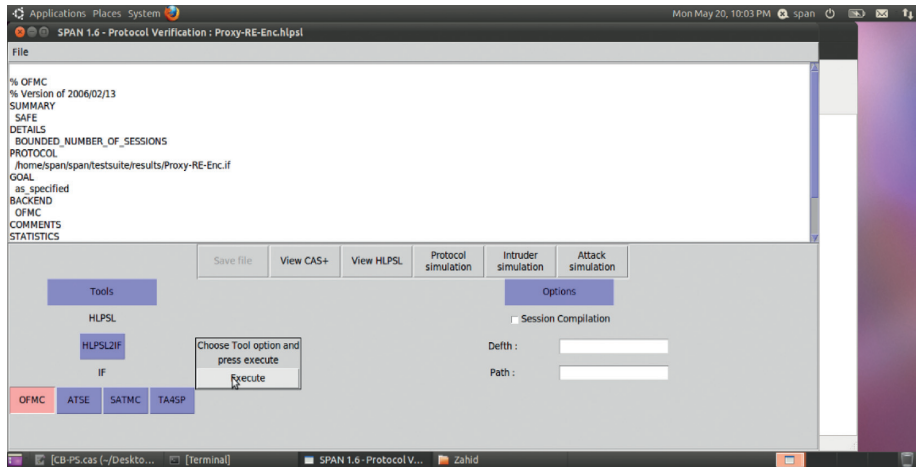


Figure 7: OFMC results.

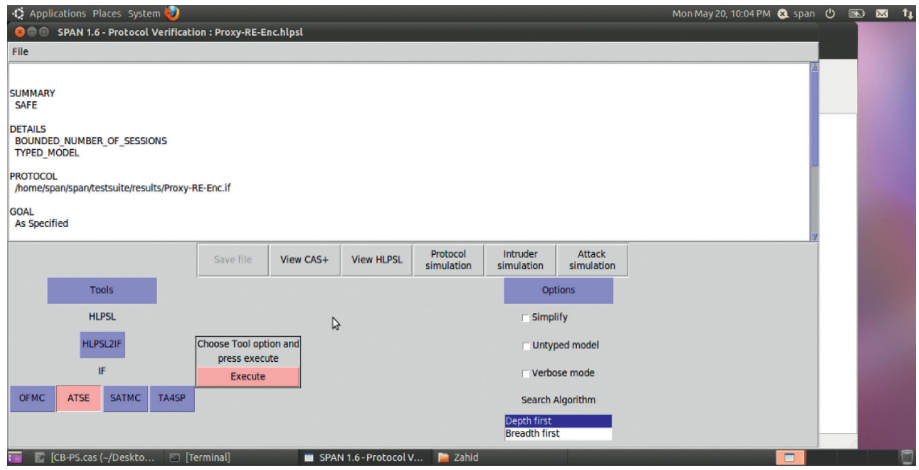


Figure 8: ATSE results.

Table 5: HLPSL code for the producer.

```
Role role_Producer(Edgeservicerouter:agent, Producer:agent, Consumer:agent, Pbpr:pub
lic_key,Pbcr:public_key,SND,RCV:channel(dy)) played_by Producer def = local State:= 0
      State:nat,Lfk:symmetric_key,Encrypt:hash_func,Npr:text,Cnt:text  init
      transition
1.  State =0 /\ RCV(start) = |> State':= 1 /\
SND(Producer.Consumer)
2.  State = 1 /\ RCV(Consumer.{Npr'}_Pbpr) = |> State':= 2 /\ Lfk':= new() /\ Cnt':= new() /\
secret(Cnt',sec_2,{Producer}) /\
witness(Producer, Edgeservicerouter, auth_1,Cnt') /\
SND(Producer.{Encrypt(Npr'.Cnt')}_Lfk') end role
```

Table 6: HLPSL code for the edge service router.

```
Role role_Edgeservicerouter(Secondlastnode:agent, Producer:agent, Consumer:agent,Pbp
r:public_key,Pbcr:public_key,SND,RCV:channel(dy)) played_by Secondlastnode def = local
          State:nat,Lfk:symmetric_key,Cnt:text, Omega:symmetric_key,Encrypt:h ash_func,C1:text,Npr:text  init
                State:  =  0  transition
3. State = 0 /\ RCV(Producer.{Encrypt(Npr'.Cnt')}_Lfk') = |> State':= 1 /\
request(Edgeservicerouter,Producer,auth_1,Cnt') /\ secret(Cnt',sec_2,{Producer}) /\ Omega':= new() /\ C1':= new() /\
secret(Cpr',sec_4,{Consumer}) /
witness(Edgeservicerouter, Consumer,auth_3,C1′)  /\
SND(Secondlastnode.{Encrypt(C1'.Npr')}_Omega') end role
```

Table 7: HLPSL code for the consumer.

```
Role role_Consumer(Edgeservicerouter:agent, Producer:agent, Consumer:agent, Pbpr:pub
lic_key,Pbcr:public_key,SND,RCV:channel(dy)) played_by Consumer def = local
State:nat,Omega:symmetric_key,Encrypt:hash_func,Cpr:text,Npr:text init State:= 0 transition
                1. State = 0 /\ RCV(Producer.Consumer) = |> State':= 1 /
Npr':= new() /\ SND(Consumer.{Npr'}_Pbpr)
            7. State = 1 /\ RCV(Edgeservicerouter.{Encrypt(Cpr'.Npr)}_Omega') = |> State':= 2 /\
secret(Cpr',sec_4,{Consumer}) end role
```

Table 8: HLPSL code for the session.

```
Role
session1(Edgerouternode:agent, Producer:agent,Consumer:agent, Pbpr:public_k ey,Pbcr:public_key) def =
      local
          SND3,RCV3,SND2,RCV2,SND1,RCV1:channel(dy)  composition
role_Edgerouternode(Edgerouternode, Producer,Consumer, Pbpr,Pbcr,SND3, RCV3) /\ role_Consumer(Edgerouternode,
Producer,Consumer, Pbpr,Pbcr,SND2,RCV2) /\ role_Producer(Edgerouternode, Producer,Consumer, Pbpr,Pbcr,SND1,RCV1) end
 role
session2 Edgerouternode:agent, Producer:agent, Consumer:agent, Pbpr:public_k ey,Pbcr:public_key) def =
      local
          SND1,RCV1:channel(dy)  composition
role_Producer(Edgerouternode, Producer,Consumer, Pbpr,Pbcr,SND1,RCV1) end role
```

Lee and Han's 2 [24], Wang et al.'s [25], Srinivasan and Rangan's [22], Bhatia et al.'s [17], and Wang et al.'s [13] existing schemes.

*6.2. Communication Overhead.* The term communication overhead in the computer network refers to how much time the communication channel spends to send a single message. It is directly proportional to how long is your message. It means that how much extra bits will be sent along with the actual message. Further, it depends on the scheme that is implemented for desired network communication. Now here, we compare our proposed scheme with the existing schemes, i.e., Xu et al.'s [20], Guo et al.'s [23], Lee and Han's [24], Wang et al.'s [25], Srinivasan and Rangan's [22], Bhatia et al.'s [17], and Wang et al.'s [13], with respect to communication overheads and illustrate that how much communication overhead is reduced by the proposed scheme. We accept that $|G2| \cong |G1| \cong |G| \cong 1024$ bits, $|P| \cong 1024$ bits, $|q| \cong 160$ bits, $|n| \cong 80$ bits, and $|\mathcal{M}| = 1024$ bits, respectively. The required communication overhead by Xu et al.'s scheme [20] is $2|\mathcal{M}| + 7|G| = 9216$, by Guo et al.'s scheme [23] is $2|\mathcal{M}| + 6|G| = 8192$, by Lee and Han's scheme 1 [24] is $2|\mathcal{M}| + 4|P| = 6144$, by Lee and Han's scheme 2 [24] is $2|\mathcal{M}| + 6|P| = 8192$, by Wang et al.'s scheme [25] is $2|\mathcal{M}| + 4|P| = 6144$, by Srinivasan and Rangan's scheme [22] is $2|\mathcal{M}| + 8|P| = 10240$, by Bhatia

Table 9: HLPSL code for the environment.

```
Role environment() def =
        const
        hash_0:hash_func,pbr:public_key,alice:agent, producer:agent,bob:age
nt,pbcr:public_key,const_1:agent, const_2:agent, const_3:public_key,const_
4:public_key,auth_1:protocol_id,sec_2:protocol_id,auth_3:protocol_id,sec
_4:protocol_id
        intruder_knowledge = {alice,bob,producer}       composition
                session2(const_1,i,const_2,const_3,const_4)
session1(producer, alice,bob,pbr,pbcr) end role goal
   authentication_on auth_1 secrecy_of sec_2 authentication_on auth_3
secrecy_of sec_4 end goal environment()
```

et al.'s scheme [17] is $2|\mathcal{M}| + 6|q| = 3008$, by Wang et al.'s scheme [13] is $2|\mathcal{M}| + 7|G| = 9216$, and for the proposed scheme is $2|\mathcal{M}| + 6|n| = 2528$, respectively. Moreover, we achieve that the proposed scheme is 9216–2528/$9216 * 100 = 72.569\%$ faster than that in [20], 8192–2528/$8192 * 100 = 69.140\%$ faster than that in [23], 6144–2528/$6144 * 100 = 58.854\%$ faster than that in [24] (for 1), 8192–2528/$8192 * 100 = 69.140\%$ faster than that in [24] (for 2), 6144–2528/$6144 * 100 = 58.854\%$ faster than that in [25], 10240–2528/$10240 * 100 = 75.312\%$ faster than that in [22], 3008–2528/$3008 * 100 = 15.957\%$ faster than that in [17], and 9216–2528/$9216 * 100 = 72.569\%$ faster than that in [13], respectively. As a result, from the abovementioned findings, our proposed scheme is faster than the recent research scheme [13] up to 72.569%; Figure 5 illustrates the differentiation.

## 7. Conclusion

The access control management faces high security issues in CCN at the time, when the content provider distributes the contents within the network. For this purpose, we address a secure content architecture for access control in CCN known as CPRES. The proposed CPRES believes on four basic parties on the network, i.e., producer, KGC, edge service router, and consumer. When the consumer (one of the basic element) retrieves encrypted content from the edge service router, he/she just contacts with KGC instead of the producer to authenticate themselves and fetch keys for content decryption. Our scheme accurately fulfils the security requirements, i.e., confidentiality L-1 and L-2 encryption, and replay attacks. Also, the CL-PRE plays a unique role to generate partial keys for improving the security of content accessing, showing that the proposed scheme reduced the computational and communication cost as compared to the existing schemes up to 58.4% to 93.80% and 15% to 72.569%, respectively. So, the proposed CPRES is more attractive to use in the resource-constrained mobile devices.

## Appendix

## Implementation and Validation Using AVISPA Tool

AVISPA is a security claim verification tool, which ensures the scheme protection, concerning two well-known attacks, called man-in-the-middle and replay. The simulation code is generally executed in $\mathcal{HLPSL}$, identified as the high-level protocol specification language. Typically, the basic architecture of the AVISPA tool is given in Figure 6. Each and every participant is usually free and contains some information in kind of guidelines for communication among other additional participants using channels. According to the architecture, the AVISPA tool first composes the code in $\mathcal{HLPSL}$ and translates it directly into an intermediate format ($\mathcal{IF}$) simply by the help of the $\mathcal{HLPSL}2\mathcal{IF}$ translator. $\mathcal{IF}$ is a further lower-level language as compared to $\mathcal{HLPSL}$ and directly read by AVISPA's backends. AVISPA is executed in four backends: (1) OFMC (on-the fly model checker), (2) CL-AtSe (constraint logic-based attack searcher), (3) SATMC (SAT-based model checker), and (4) TA4SP (tree automata based on automatic approximations for the analysis of security protocols). On the basis of these backends, the output format is created in addition to describing the result and then confirms whether or not the scheme is secure from attacks [48].

Further, this section summarizes our proposed certificateless proxy reencryption scheme based on the hyperelliptic curve for access control in CCN roles in a recognized security simulation tool known as AVISPA. The proposed scheme algorithm is written in the $\mathcal{HLPSL}$ language for checking the validation of security attacks through two backends of the AVISPA tool, i.e., OFMC and ATSE. The simulation results are fully safe against these two backends from the intruder's attack that are shown in Figures 7 and 8. The $\mathcal{HLPSL}$ code has five roles in our proposed algorithm. To understand these roles in the $\mathcal{HLPSL}$ code it is undermined that the symbols used in the proposed algorithm are shown after the arrow symbol ($\leftrightarrow$) and the $\mathcal{HLPSL}$ code symbols are shown before the arrow symbol. So, in Table 5, in the producer role, $Lfk \leftrightarrow Lfk$,Encrypt $\leftrightarrow \oplus$, Npr $\leftrightarrow$ Npr, Cnt $\leftrightarrow$ CNT,{Encrypt (Npr'.Cnt')}$\_Lfk$') $\leftrightarrow$ (CNT, Npr) $\oplus Lfk$, Pbpr $\leftrightarrow \mathcal{PB}$pr, and Pbcr $\leftrightarrow \mathcal{PB}$cr; in Table 6, in the edge service router role, Omega $\leftrightarrow \Omega$, $\mathcal{C}1 \leftrightarrow \mathcal{C}1 = \mathcal{R}.\mathcal{L}$ and {Encrypt(C1'.Npr')}_Omega') $\leftrightarrow \mathcal{C}1^* = \mathcal{C}1 \oplus \Omega$. Similarly, Tables 7–9 provide the $\mathcal{HLPSL}$ code for the consumer role, session role, and environment role, respectively. The symbols of Tables 7–9 are already explained above. Further, the consumer role handles the decryption operations. The session role determines how many sessions are made among the nodes. The environment's role is generally related to security of the desired algorithm. Finally, in Figures 7 and 8, the simulation results for the proposed scheme illustrate that our scheme gives fully safe results

against the two backends, OFMC and ATSE, of the AVISPA tool.

## Data Availability

The data used to support the findings of this study are uploaded to the GitHub repository (xx).

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

## Acknowledgments

This project was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant no. (DF-459-156-1441). The authors, therefore, gratefully acknowledge the DSR technical and financial support.

## References

[1] C. Fang, H. Yao, Z. Wang, W. Wu, X. Jin, and F. R. Yu, "A survey of mobile information-centric networking : research issues and challenges," vol. 20, no. 3, pp. 2353–2371, 2018.

[2] K. Xue, X. Zhang, Q. Xia, D. S. L. Wei, H. Yue, and F. Wu, "SEAF: a secure, efficient and accountable Access control framework for information centric networking," in *Proceedings of the IEEE Computer and Communications*, pp. 2213–2221, Honolulu, HI, USA, April 2018.

[3] J. Kuriharay, E. Uzun, and C. A. Wood, "An encryption-based access control framework for content-centric networking," in *Proceedings of the 2015 IFIP Networking Conference (IFIP Networking)*, Toulouse, France, May 2015.

[4] E. G. Abdallah, H. S. Hassanein, and M. Zulkernine, "A survey of security attacks in information-centric networking," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1441–1454, 2015.

[5] S. Siddiqui, A. Waqas, A. Khan, F. Zareen, and M. N. Iqbal, "Congestion controlling mechanisms in content centric networking and named data networking-a survey," in *Proceedings of the 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, Sukkur, Pakistan, January 2019.

[6] A. Boukerche and R. W. L. Coutinho, "LoICen: A novel location-based and information-centric architecture for content distribution in vehicular networks," *Ad Hoc Networks*, vol. 93, Article ID 101899, 2019.

[7] Q. Zheng, G. Wang, R. Ravindran, and A. Azgin, "Achieving secure and scalable data access control in information-centric networking," in *Proceedings of the 2015 IEEE International Conference on Communications (ICC)*, pp. 5367–5373, London, UK, June 2015.

[8] I. U. Din, B. S. Kim, S. Hassan, M. Guizani, M. Atiquzzaman, and J. Rodrigues, "Information-centric network-based vehicular communications : overview and research opportunities," *Sensors*, vol. 18, no. 1, p. 3857, 2018.

[9] B. Ahlgren, C. Dannewitz, C. Imbrenda, and D. Kutscher, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, 2012.

[10] C. Cavanagh and U. C. Irvine, UC Irvine Electronic Theses and Dissertations, vol. 228, 2016.

[11] C. Zhou, Z. Zhao, W. Zhou, and Y. Mei, "Certificateless key-insulated generalized signcryption scheme without bilinear pairings," *Security and Communication Networks*, vol. 2017, Article ID 8405879, 17 pages, 2017.

[12] A. Rahman, I. Ullah, M. Naeem et al., "A lightweight multi-message and multi-receiver heterogeneous hybrid signcryption scheme based on hyper elliptic curve," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 5, pp. 160–167, 2018.

[13] Q. Wang, W. Li, and Z. Qin, "Proxy Re-encryption in access control framework of information-centric networks," *IEEE Access*, vol. 7, pp. 48417–48429, 2019.

[14] M. Green and G. Ateniese, "Identity-based proxy re-encryption," *Applied Cryptography and Network Security*, Springer, Berlin, Heidelberg, Germany, 2007.

[15] L. Wang, L. Wang, M. Mambo, and E. Okamoto, "New identity-based proxy Re-encryption schemes to prevent collusion attacks," in *Proceedings of the International Conference on Pairing-Based Cryptography*, Beijing, China, 2010.

[16] L. L. Wang, K. F. Chen, X. P. Mao, and Y. T. Wang, "Efficient and provably-secure certificateless proxy re-encryption scheme for secure cloud data sharing," *Journal of Shanghai Jiaotong University*, vol. 19, no. 4, pp. 398–405, 2014.

[17] T. Bhatia, A. K. Verma, and G. Sharma, "Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud," *Transactions on Emerging Telecommunications Technologies*, vol. 29, no. 6, Article ID e3309, 2018.

[18] C. A. Wood and E. Uzun, "Flexible end-to-end content security in CCN," in *Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference (CCNC)*, pp. 858–865, Las Vegas, NV, USA, January 2014.

[19] M. Mangili, F. Martignon, and S. Paraboschi, "A cache-aware mechanism to enforce confidentiality, trackability and access policy evolution in content-centric networks," *Computer Networks*, vol. 76, pp. 126–145, 2015.

[20] L. Xu, X. Wu, and X. Zhang, "Cl-PRE," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, New York, NY, USA, May 2012.

[21] M. Ion, J. Zhang, and E. M. Schooler, "Toward content-centric privacy in ICN: attribute-based encryption and routing," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, p. 513, 2013.

[22] A. Srinivasan and C. P. Rangan, "Certificateless proxy re-encryption without pairing," in *Proceedings of the 3rd International Workshop on Security in Cloud Computing*, pp. 41–52, Dubai, 2015.

[23] H. Guo, Z. Zhang, J. Zhang, and C. Chen, "Towards a secure certificateless proxy re-encryption scheme," in *Proceedings of the International Conference on Provable Security*, pp. 330–346, Melaka, Malaysia, October 2013.

[24] H. S. Lee and D. G. Han, "Information security and cryptology-ICISC 2013," in *Proceedings of the International Conference on Information Security and Cryptology*, pp. 67–88, Seoul, Korea, December 2014.

[25] Y. Wang, H. Xiong, S. Argamon, X. Y. Li, and J. Z. Li, "Big data computing and communications," in *Proceedings of the First International Conference, BigCom 2015*, pp. 205-206, Taiyuan, China, August 2015.

[26] R. Tourani, S. Misra, T. Mick, and G. Panwar, "Security, privacy, and access control in information-centric networking: a survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 556–600, 2018.

[27] K. Fu, S. Kamara, and T. Kohno, "Key regression: enabling efficient key distribution for secure distributed storage," vol. 149, 2006 Comput. Sci. Dep. Fac. Publ. Ser.

[28] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 127–144, Konstanz, Germany, May 1998.

[29] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," *ACM Transactions on Information and System Security*, vol. 9, no. 1, pp. 1–30, 2006.

[30] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *Proceedings of the 14th ACM conference on Computer and Communications Security*, Alexandria, VA, USA, 2007.

[31] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in *Proceedings of the IACR International Conference on Public-Key Cryptography*, pp. 360–379, Barcelona, Spain, March 2008.

[32] R. H. Deng, J. Weng, S. Liu, and K. Chen, "Chosen-ciphertext secure proxy re-encryption without pairings," in *Proceedings of the International Conference on Cryptology and Network Security*, pp. 1–17, Hong Kong, China, December 2008.

[33] X. A. Wang, J. Ma, and X. Yang, "A new proxy re-encryption scheme for protecting critical information systems," *Journal of Ambient Intelligence and Humanized Computing.*vol. 6, no. 6, pp. 699–711, 2015.

[34] H. Shacham, "A cramer-shoup encryption scheme from the linear assumption and from progressively weaker linear variants," 2007.

[35] Y. Ren, D. Gu, S. Wang, and X. Zhang, "Hierarchical identity-based proxy re-encryption without random oracles," *International Journal of Foundations of Computer Science*, vol. 21, no. 6, pp. 1049–1063, 2010.

[36] L. Batten, G. Li, W. Niu, and M. Warren, "Applications and techniques in information security," in *Proceedings of the International Conference on Applications and Techniques in Information Security*, Melbourne, VIC, Australia, November 2014.

[37] Q. Tang, P. Hartel, and W. Jonker, "Inter-domain identity-based proxy re-encryption," in *Proceedings of the International Conference on Information Security and Cryptology*, pp. 332–347, Beijing, China, December 2009.

[38] T. Mizuno and H. Doi, "Secure and efficient IBE-PKE proxy re-encryption," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E94-A, no. 1, pp. 36–44, 2011.

[39] J. Shao and Z. Cao, "Multi-use unidirectional identity-based proxy re-encryption from hierarchical identity-based encryption," *Information Sciences*, vol. 206, pp. 83–95, 2012.

[40] K. Liang, Z. Liu, X. Tan, D. S. Wong, and C. Tang, "A CCA-secure identity-based conditional proxy re-encryption without random oracles," in *Proceedings of the International Conference on Information Security and Cryptology*, pp. 231–246, Seoul, Korea, November 2013.

[41] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Proceedings of the European Symposium on Research in Computer Security*, pp. 257–272, Luxembourg, Luxembourg, September 2014.

[42] S. Saxby, "Communications and multimedia security," *Computer Law & Security Review*, vol. 22, no. 4, p. 338, 2006.

[43] Y. Zheng, S. Tang, C. Guan, and M. R. Chen, "Cryptanalysis of a certificateless proxy re-encryption scheme," in *Proceedings of the 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies*, pp. 307–312, Xi'an, China, September 2013.

[44] S. A Ullah, "Review of signcryption schemes based on hyper elliptic curve," in *Proceedings of the 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)*, Chengdu, China, August 2017.

[45] Nizamuddin, C. Shehzad Ashraf, and N. Amin, "Signcryption schemes with forward secrecy based on hyperelliptic curve cryptosystem," in *Proceedings of the 8th International Conference on High-capacity Optical Networks and Emerging Technologies*, pp. 244–247, Riyadh, Saudi Arabia, December 2011.

[46] A. J. Ordonez, R. P. Medina, and B. D. Gerardo, "Modified El gamal algorithm for multiple senders and single receiver encryption," in *Proceedings of the 2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, Malaysia, April 2018.

[47] I. Ullah, N. Amin, J. Khan et al., "A novel provable secured signcryption scheme PSSS: a hyper-elliptic curve-based approach," *Mathematics*, vol. 7, no. 8, p. 686, 2019.

[48] R. Ali and A. K. Pal, "Three-factor-based confidentiality-preserving remote user authentication scheme in multi-server environment," *Arabian Journal for Science and Engineering*, vol. 42, no. 8, pp. 3655–3672, 2017.