Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4215441, 11 pages
https://doi.org/10.1155/2022/4215441

Research Article

An Efficient Online/Offline Signcryption Scheme for Internet of Things in Smart Home

Nayab,[1] **Saddam Hussain**,[1] **Amerah Alabrah**,[2] **Syed Sajid Ullah**,[3] **Hizbullah Khattak**,[1] **Taha M. Alfakih**,[4] **and Insaf Ullah**[5]

[1]*Department of Information Technology, Hazara University Mansehra, 21120, K-P, Pakistan*
[2]*Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia*
[3]*Department of Information and Communication Technology, University of Agder (UiA), N-4898 Grimstad, Norway*
[4]*Faculty of Engineering and Information Technically, Aljanad University for Science and Technology, Taiz, Yemen*
[5]*Hamdard Institute of Engineering & Technology, Islamabad 44000, Pakistan*

Correspondence should be addressed to Saddam Hussain; saddamicup1993@outlook.com, Syed Sajid Ullah; syed.s.ullah@uia.no, and Taha M. Alfakih; talfakih@just.edu.ye

Received 10 February 2022; Accepted 24 March 2022; Published 29 April 2022

Academic Editor: Kuruva Lakshmanna

The delivery of unified intelligent services is accomplished through a networked environment comprised of a wide array of electronic devices. Through the use of Internet of Things (IoT) technology, smart homes collect data from their surroundings and use it to improve their tenants' lives. Remote control, real-time monitoring, and a fire alarm are all characteristics of smart home security. Since smart homes hold personally identifying information about their residents, security is critical to ensure their reliability and prevent data breaches. In this paper, a certificateless online/offline signcryption (COOS) technique for IoT-enabled smart homes is proposed. The proposed solution takes advantage of a resource-constrained smart home device–friendly algorithm known as the Hyperelliptic Curve Cryptosystem (HCC). The suggested approach satisfies the security requirements of unforgeability, confidentiality, resistance to replay attacks, and non-repudiation. The complexity analysis in terms of communicational and computational costs demonstrates the efficiency of the proposed scheme. Finally, we validate the security against Man-In-The-Middle-Attack (MITM) and anti-reply attacks using Automated Validation of Internet Security Protocols and Applications (AVISPA). The data imply that the recommended course of action is safe.

1. Introduction

An essential part of the IoT, smart homes rely on IoT to effectively serve customers by communicating with a variety of digital devices. IoT-based smart home technology has transformed human lives by providing connectivity to everyone irrespective of place and time [1–3]. In recent years, home automation systems have become more sophisticated. These systems provide basic facilities and methods for transferring all types of device information and services.

The Internet of Things is a world of actuators and sensors embedded in the material that is connected to a wireless and wired network that is permanent and interactive. The theme of the Internet of Things is to access and control these smart devices. The use of the Internet of Things by smart homes has made users' lives more creative and comfortable [4, 5]. Figure 1 shows a typical smart home model, which includes appliances, actuators, sensors, and controllers. The controller monitors the sensor data and sends signals to the other linked sensors or electronic equipment, instructing them on how to operate appropriately. Apart from intelligence, security is a major issue in smart homes, as devices are connected to the internet, requiring more secure communication [6].

The significant ingredients of the smart home include entrance security, remote control, real-time monitoring, and fire alarm. As the sensitive data of the user is stored in smart homes, so security needs to be considered to ensure reliability to protect customers' data from the breach.

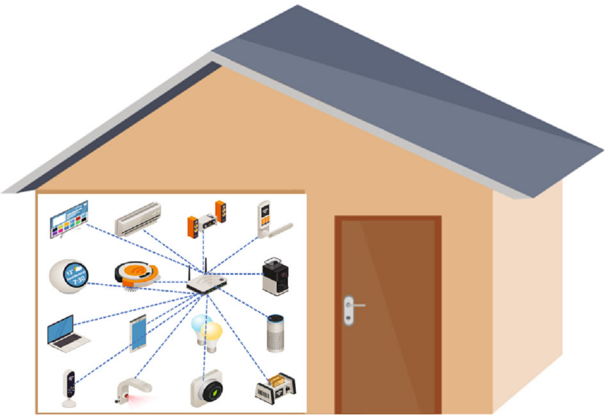


Figure 1: Generic illustration of smart home.

Authenticity and security of data are essential for data because of public access. Authenticity can be gained using digital signatures [7, 8], while data confidentiality can be obtained using encryption [9].

Unfortunately, the higher computational and communicational cost of the signature and encryption opens up the way to signcryption. In 1997, Zheng [10] presents the concept of signcryption, which integrates the functionality of digital signature and encryption simultaneously. As the collected data from the Internet of Things can be accessible to a number of people, therefore, sensitive personal information in smart homes rises some dangerous security questions. In this regard, a number of cryptographic techniques have been present in literature, i.e., PKI, IBC and CLC [11]. The revocation and distribution of certificates are two challenges that have an impact on PKI. In addition, IBC is plagued by a crippling issue with key escrow. Therefore, CLC is the most appropriate solution available for smart home communication systems [12]. In addition, a few CLC solutions for the smart home have been found in the past, but the proposed schemes suffer from the use of heavy computational and communicational needs. Therefore, in this paper, we are suggesting a new solution for securing smart home communication at the expense of minimal resources. The major contributions of our research are given below:

(i) We propose an online/offline certificateless signcryption scheme for smart home communication using a lightweight HCC

(ii) The proposed scheme is capable of achieving security necessities such as integrity, confidentiality, anti-replay attack, and non-repudiation

(iii) We perform a detailed comparison in terms of communicational and computational costs. The comparison result reveals that the suggested technique is more efficient and secure than previous online/offline signcryption schemes

(iv) Finally, we validate the security of the designed scheme using AVISPA. The results show that the intended scheme is secure against security attacks

1.1. Road Map of the Article. The rest of the paper is organized as follows: Section 2 presents the related work. The essential prerequisites for the proposed scheme are discussed in Section 3. The proposed network model is described in Section 4. In Section 5, we compared the proposed scheme to other schemes that have already been implemented. Conclusions are presented in Section 6. The simulation data and code is placed in the appendix section.

2. Related Work

A smart home brings a very comfortable and intelligent life to its customers. Recently, smart home communication gains too much popularity due to a large number of data connections. Replay and mobile theft, for example, can expose user privacy and information to a range of attacks. Furthermore, the authenticity and security of communication in smart homes is critical. Additionally, smart home devices require a smart home server to undertake heavy activities for them due to resource constraints. Therefore, in order to meet the above requirement, you may need an online/offline technique. Thus, Luo et al. [13] present the first CLC-based online/offline signcryption for IoT. The authors claim that the designed scheme is provable secure under the computational model of Random Oracle (ROM). However, Luo et al.'s technique was determined to be insecure against private key compromise [14]. In addition, the authors use bilinear pairing for security hardness which makes the given scheme inefficient due to heavy pairing operations. Later, Li et al. [15] propose a new certificateless online/offline approach utilizing bilinear pairing under the computational model of Random Oracle, though the authors did not propose application deployment of the suggested scheme. In addition, the complexity design scheme is entirely based on bilinear pairing. In 2017, Li et al. [16] threw a certificateless online/offline approach utilizing bilinear pairing for the Internet of Things under computational model of Random Oracle. However, the complexity of Li et al. is entirely based on bilinear pairing. Rao [17] introduces an attribute-based online/offline signcryption (AOOS) technique utilizing bilinear pairing under the computational model of Random Oracle. Nonetheless, they did not present an application deployment of the design scheme. In addition, the complexity of [17] is entirely based on bilinear pairing. Saeed et al. [18] presented a heterogeneous online/offline signcryption scheme for wireless sensor networks that operates on ROM. However, the given scheme is constructed based on bilinear pairing. In 2019, Iqbal et al. [19] propose a blockchain-based AOOS strategy for wireless sensor networks. Unfortunately, the proposed strategy is based on bilinear pairing.

Using the complexity of bilinear pairing, Yosef and Mahmoud [20] proposed an identity-based signcryption approach to secure end-user connections in smart home communication. Unfortunately, because of the use of identity-based signcryption, the design scheme suffers from a key escrow problem. Furthermore, the proposed system is built using bilinear pairing, that make it inefficient for smart homes devices.

In 2018, Sai et al. [21] introduce an effective certificateless online/offline signcryption scheme that can offer biometric authentication for user identity. Regrettably, the proposed approach is based on bilinear pairing.

3. Preliminaries

3.1. Hyperelliptic Curve Cryptosystem (HCC). HCC is an extension of elliptic curve cryptography (ECC), a public key cryptography approach that is comparable to ECC and bilinear pairing. In comparison to other approaches such as ECC, RSA, and digital signature algorithm (DSA), the HCC gives the same level of security. HCC is a suitable solution for resource-constrained applications due to its small key size. The HCDLP contributes to the security of HCC by preventing an adversary from cracking the keys even if the P and Q are publicly available.

3.1.1. Hyperelliptic Curve Discrete Logarithm Problem (HCDLP). The following complexity assumptions have been made in reference to the HCDLP:

(i) Let $\theta \mathscr{E} \{1, 2, 3, \cdots, (\mathrm{y} - 1)\}$ and $\mathscr{X} = \theta.\mathscr{D}$; then, finding θ from $\mathscr{X}$ is called HCDLP

3.2. Threat Model. A threat in computing infrastructure is an incident that has the potential to harm or destroy the system. Threats are mostly events that aim to compromise a computing infrastructure's integrity, confidentiality, and availability. Some system flaws, such as configuration design errors and security vulnerabilities, might lead to such dangers. Thus, anyone with evil purpose and technical competence can use these vulnerabilities to attack them, exposing the risks.

Typically, cryptographic techniques are designed to work in an open environment where attackers can retrieve information shared between peers. The Doley-Yao threat model is frequently used in the development of such security solutions [22]. This model posits an insecure public channel (making information entities untrustworthy) and powerful adversaries, participants, and other organizations capable of receiving network messages. Despite the adversaries' skills, there is knowledge that is off-limits. This information could be used to decrypt the message, encrypt the plaintext, or generate the same HMAC value without the right key by guessing random integers from some sample space. As a result, the Doley-Yao threat model is used in the design of the proposed approach in this paper, and the sole KGC is regarded entirely dependable.

4. Proposed Scheme

In this section, we will discuss the proposed network model its mathematical construction.

4.1. Design Network Model. In Figure 2, we demonstrated the designed network model for smart home communication using certificateless online/offline signcryption scheme with the complexity based on HCC. The designed network model has the following entities:

(ii) Key generation center: It is a reliable party that is responsible for establishing secure communication between sender, controller, and receiver

(iii) Sender: The sender can be any smart device that can sense/collect data such as Lamp, smartphone, TV, AC, and CCTV

(iv) Receiver: The receiver can be any smart device that can receive data/messages such as smartphone, server, and PC

(v) Controller: The controller is a home gateway device that is able to connect and control the smart communication home

It is necessary to connect the smart home devices to the KGC in order to create secure communication. In the proposed network paradigm, the KGC is in charge of creating a partial private key, master keys, and a set of public parameters, respectively. The KGC then retained possession of the master secret key and distributes the remaining data throughout the network. This can be used by both the sender and the recipient to produce their own public and private keys for use in secure communication.

4.2. Construction of the Designed Scheme. In this section, we will construct a certificateless online/offline signcryption for smart home communication by using the following steps [23]. Furthermore, the notations used in the designed algorithm are added in Table 1.

4.3. Setup. Firstly, a security parameter ($\mathscr{k}$) is given to the key generation center (KGC). After that, the KGC choose three hash functions $(H_o, H_p, \text{and}\, H_q)$. Furthermore, the KGC pick $l \epsilon \{1, 2, \cdots.., n-1\}$ as a master secret key and compute the corresponding master public key as $\mathscr{W} = l.\mathscr{D}$. Finally, the KGC announce $\sigma = \{\mathscr{W}, \mathscr{D}, H_o, H_p, \text{and}\, H_q\}$ publically as open parameter set.

4.4. Key Generation. Here in this phase, the participant registers themselves with KGC by sending their identity (ID_p). Upon receiving the ID_p, the KGC then picks $\eta_p \epsilon \{1, 2, \cdots.., n-1\}$, computes $\Gamma_p = \eta_p.\mathscr{D}$, calculates $\mathscr{Z}_p = \eta_p + l.H_o(ID_p, \Gamma_p)$, and sends $\mu = (\Gamma_p, \mathscr{Z}_p)$ to the participant with ID_p. So, after reception, a participant $\vartheta_p \epsilon \{1, 2, \cdots.., n-1\}$ as a secret parameter and makes $X_p = \vartheta_p.\mathscr{D}$. The participant then sets $\mathscr{V}_p = (\vartheta_p, \mathscr{Z}_p)$ as the private key and as $\mathscr{Q}_p = (\Gamma_p, X_p)$ as a public key.

4.5. Signcryption. The signcryption phase is divided into two parts; the online part and the online part:

(i) Offline part: The signer selects $\mathscr{a} \epsilon \{1, 2, \cdots.., n-1\}$, computes $\mathscr{S} = \mathscr{a}.\mathscr{D}$, calculates $r_1 = H_o(ID_r, \Gamma_r)$, computes $r_2 = H_p(ID_s, ID_r, X_s, X_r, \mathscr{S}, m)$, and $\mathscr{K} = (r_1 + \Gamma_r + X_p)$, respectively

(ii) Online part: It computes $\mathscr{w} = (m, Ns) \oplus H_q(\mathscr{K})$ and $\mathscr{N} = (\vartheta_s + \mathscr{a})/(r_2 + \vartheta_s + \mathscr{Z}_s)$ and finally sends $\psi = (\mathscr{N}, \mathscr{w}, \mathscr{S}, r_2)$ to the intended receiver

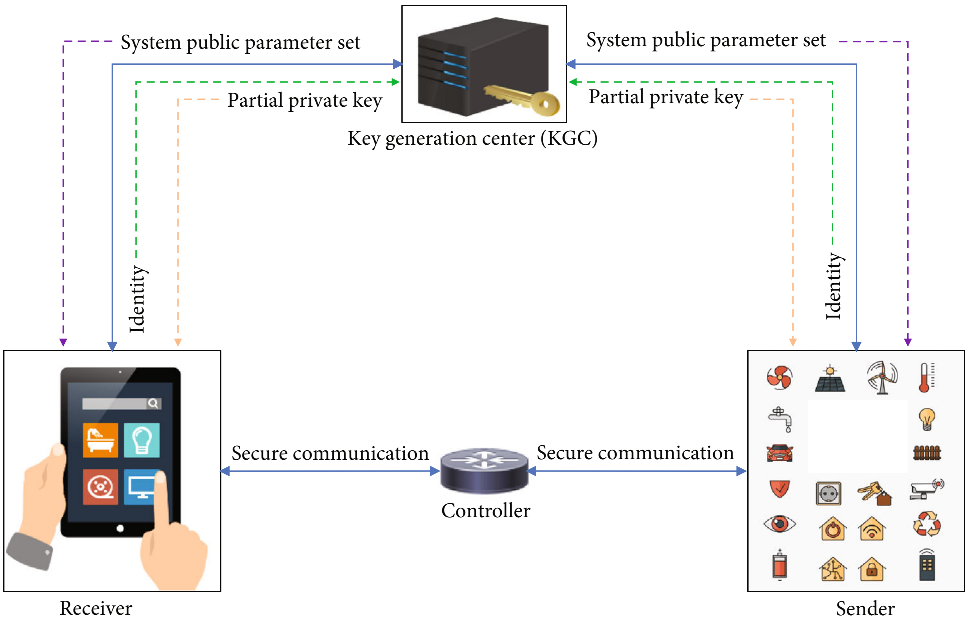


Figure 2: Designed network model.

Table 1: Symbols used in the designed algorithm.

S/N	Symbol	Explanation
1	KGC	Key generation center
2	$\mathscr{k}$	Security parameter
3	l	Private key of KGC
4	H_o, H_p, H_q	Hash functions
5	$\mathscr{D}$	Divisor of HCC
6	$\mathscr{W}$	Master public key of KGC
7	ϑ_p	User partial private key
8	ID_p	Identity of both users (sender and receiver)
9	$\mathscr{Q}_p$	User public key
10	$\mathscr{V}_p$	User private key
11	ψ	Signcrypted text

4.6. Unsigncryption. After receiving the signcrypted text ψ, the receiver performs the following computations:

(i) Compute $\mathscr{K} = \mathscr{S}(\vartheta_r + \mathscr{Z}_r)$, and uncover the plaintext as $(m, Ns) = \mathscr{w} \oplus H_q(\mathscr{K})$

(ii) Compute $r_2{}' = H_p(ID_s, ID_r, X_s, X_r, \mathscr{S}, m)$, and if $r_2{}' = r_2$, accept the signcrypted text ψ; otherwise, reject

4.7. Correctness. The recipient of the message can verify and decrypt the received $\psi = (\mathscr{N}, r_2)$ by doing the following steps.

It first uncovers the secret key by performing the computations as follows: $\mathscr{K} = (\vartheta_r + \mathscr{Z}_r) = \mathscr{a}.\mathscr{D}(\vartheta_r + \eta_r + l.H_o(ID_r, \Gamma_r)) = \mathscr{a},(\vartheta_r.\mathscr{D} + \eta_r.\mathscr{D} + l.\mathscr{D}\,H_o(ID_r, \Gamma_r)) = \mathscr{a}$, and $(\Gamma_r + X_r + \mathscr{W}.r_1) = \mathscr{K}$; then, it recovers the plaintext as follows: $(m, Ns) = \mathscr{w} \oplus H_q(\mathscr{K})$, and compute $r_2{}' = H_p(ID_s, ID_r, X_s, X_r, \mathscr{S}, m)$, and if $r_2{}' = r_2$, then accept ψ; otherwise, reject it.

5. Security Analysis

In this section, we present the security analysis of the designed scheme.

5.1. Confidentiality. When the attacker is unable to extract the original message from the ciphertext, then the phenomenon is known confidentiality. In the designed scheme the sender of the message first generates an encryption key $\mathscr{K} = (\mathscr{W}.r_1 + \Gamma_r + X_r)$ by utilizing private information such as $\mathscr{a}$; then using the secret $\mathscr{K}$, it simply encrypts the message as $\mathscr{w} = (m, Ns) \oplus H_q(\mathscr{K})$. Thus, when the attacker wants to uncover (m, Ns) from $\mathscr{w}$, then the attacker needs to find $\mathscr{K}$ either from $\mathscr{K} = (\mathscr{W}.r_1 + \Gamma_r + X_r)$ or $\mathscr{K} = (\vartheta_r + \mathscr{Z}_r)$. Here, if the attacker wants to compute $\mathscr{K} = (\mathscr{W}.r_1 + \Gamma_r + X_r)$, then it first needs to extract $\mathscr{a}$ from $\mathscr{S} = \mathscr{a}.\mathscr{D}$, which infeasible for the attacker to solve the HCDLP. Also, if the attacker wants to calculate $\mathscr{K} = \mathscr{S}(\vartheta_r + \mathscr{Z}_r)$, then it uncovers $\mathscr{a}$ from $X_r = \vartheta_r.\mathscr{D}$ which is infeasible for an attacker to solve the solution equals HCDLP. Furthermore, it computes $\mathscr{Z}_r$ from $\mathscr{Z}_r = \eta_r + l.H_o(ID_r, \Gamma_r)$ which require η_r from $\Gamma_r = \eta_r.\mathscr{D}$ and l on $\mathscr{W} = l.\mathscr{D}$ which is equal to solving two times computations of HCDLP. Hence, from the aforementioned discussion, we conclude that the designed scheme achieves the security services of confidentiality.

5.2. Integrity. When the attacker is unable to alter the signcryption tuple, the phenomenon is known as integrity. In our designed scheme, the signer first creates a hash of the message: $r_2 = H_p(ID_s, ID_r, X_s, X_r, \mathscr{S}, m)$; then, it forwards the signcrypted tuples as $\psi = (\mathscr{N}, \mathscr{w}, \mathscr{S}, r_2)$ to the intended

Table 2: Computational time analysis of the proposed scheme with relevant schemes in terms of costly mathematical operations used.

Ref. no.	Signcryption	Un-Signcryption	Total mathematical operations
Saeed et al. [18]	1 EX+4 BPM	1 EX+1 BPM+2 BPO	2 EX+5 BPM+2 BPO
Iqbal et al. [19]	1 EX+2 BPM	1 EX+1 BPM+2 BPO	2 EX+3 BPM+2 BPO
Ashibani and Mahmoud [20]	3 BPM+1 BPO	4 BPO	3 BPM+5 BPO
Sai et al. [21]	1 EX+2 BPM	3 BPM+2 BPO	2 EX+5 BPM+2 BPO
Designed framework	2 HCDM	1 HCDM	3 HCDM

receiver. When the attacker wants to make changes in message m to $m^{/}$, then the attacker needs to change r_2 to $r_2{}^{/} = H_p(ID_s, ID_r, X_s, X_r, \mathcal{S}, m^{/})$ which is hard for the attacker due to nature of hash used (one way). Thus, the aforementioned discussion confirms that the designed framework provides the security services of integrity.

5.3. Non-repudiation. When the signer of the message is unable to decline from his transmitted signcrypted tuple, the phenomenon is known as non-repudiation. In the proposed scheme, the signer first produces a signature $\mathcal{N} = (\vartheta_s + \mathscr{a})/(r_2 + \vartheta_s + \mathcal{Z}_s)$ using his key pair of the private key $(\vartheta_s, \mathcal{Z}_s)$ which is directly linked with public key pair $(\varGamma_s, X_s)$.

Therefore, the KGC can simply guess by means of this information whether the signed tuple is sent by the sender or not.

Thus, the above discussion indicates that the proposed technique provides non-repudiation security services.

5.4. Unforgeability. When the attacker is not able to produce actual digital signature produce by the sender of the message, the phenomenon is known as unforgeability. In the proposed scheme, the sender of the message generates a signature $\mathcal{N} = (\vartheta_s + \mathscr{a})/(r_2 + \vartheta_s + \mathcal{Z}_s)$ using three private parameters (ϑ_s, Z_s, and $\mathscr{a}$). Therefore, when the attacker wants to make the same digital signature, then it needs to ϑ_s and $\mathscr{a}$ from $X_s = \vartheta_s.\mathcal{D}$, and compute $\mathcal{S} = \mathscr{a}.\mathcal{D}$ which is equal to solving two times computation of HCDLP and therefore infeasible for the attacker. On the other hand, the attacker also needs to compute $\mathcal{Z}_s$ from $\mathcal{Z}_s = \eta_s + l.H_o(ID_s, \varGamma_s)$, which further need η_s from $\varGamma_s = \eta_s.\mathcal{D}$ and l from $\mathcal{W} = l.\mathcal{D}$ which is also equivalent to twice the computation of HCDLP. Hence, in this way, the aforementioned discussion confirms that the newly proposed scheme provides the security services of unforgeability.

5.5. Anti-replay Attack. When the attacker is unable to relay the old captured messages, the phenomenon is known as an anti-replay attack. In the proposed scheme, the signer of the message attaches a new fresh nonce (Ns) that is encrypted with the message $\mathscr{w} = (m, Ns) \oplus H_q(\mathcal{K})$ using the secret key $\mathcal{K}$. When the attacker wants to uncover the fresh nonce (Ns) from $\mathscr{w}$, then the attacker needs to recover $\mathcal{K}$ as $\mathcal{K} = \mathscr{a}(\mathcal{W}.r_1 + \varGamma_r + X_r)$. here, if the attacker wants to compute $\mathcal{K} = \mathscr{a}(\mathcal{W}.r_1 + \varGamma_r + X_r)$, then it first needs to obtain $\mathscr{a}$ from $\mathcal{S} = \mathscr{a}.\mathcal{D}$, which is equal to solving an HCDLP. Thus, in this way, the aforementioned discussion confirms that the newly proposed scheme provides the security services of anti-replay attacks.

6. Performance Analysis

Based on computation time and communication overhead, we compared our proposed scheme to the existing schemes.

6.1. Computation Time. This section presents the comparison of the proposed framework with some relevant online/offline signcryption approaches cited [18–21] in terms of computational time with including parameters Bilinear Pairing Operations (BPO), Bilinear Pairing Multiplication (BPM), EXxponentiations (EX), and Hyperelliptic Curve Devisor Multiplication (HCDM). The running operational time of the given parameters is taken from [23–25].

(i) Running time of Hyperelliptic Curve Devisor Multiplication $(HCDM) = 0.48\, ms$

(ii) Running time of Bilinear Pairing Multiplication $(\mathcal{BPM}) = 4.31\, ms$

(iii) Running time of EXponentiations $(\mathcal{EX}) = 1.25\, ms$

(iv) Running time of Bilinear Pairing Operations $(\mathcal{BPO}) = 14.90\, ms$

Table 2 shows the computational time of the aforementioned parameters used in the proposed framework and the relevant online/offline signcryption schemes cited [18–21]. Lastly, Figure 3 and Table 3 clearly demonstrate the efficiency of the proposed framework in terms of computational time.

6.1.1. Percentage Improvement. The percentage computational time improvement can be calculated using the given formula:

$$\left(\frac{Cost \text{ of } previous\ scheme - Cost \text{ of } proposed\ scheme}{Cost \text{ of } previous\ scheme}\right) * 100. \quad (1)$$

(i) Percentage computational time improvement from Saeed et al. [18] is

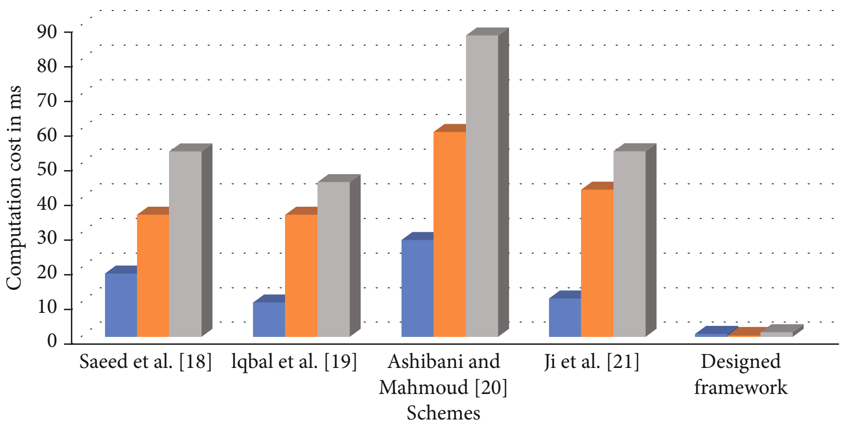


Figure 3: Computational time analysis of the proposed scheme with relevant schemes in terms of milliseconds.

Table 3: Total computational time analysis of the proposed scheme with relevant schemes in terms of milliseconds (ms).

Ref. no.	Signcryption	Un-signcryption	Total computation time
Saeed et al. [18]	18.49 ms	35.36 ms	53.85 ms
Iqbal et al. [19]	9.87 ms	35.36 ms	45.23 ms
Ashibani and Mahmoud [20]	27.83 ms	59.6 ms	87.43 ms
Sai et al. [21]	11.12 ms	42.73 ms	53.85 ms
Designed framework	0.96 ms	0.48 ms	1.44 ms

$$= \left(\frac{53.85 - 1.44}{53.85}\right) * 100 = 97.32\% \tag{2}$$

(ii) Percentage computational time improvement from Iqbal et al. [19] is

$$= \left(\frac{45.23 - 1.44}{45.23}\right) * 100 = 96.81\% \tag{3}$$

(iii) Percentage computational time improvement from Ashibani and Mahmoud [20] is

$$= \left(\frac{87.43 - 1.44}{87.43}\right) * 100 = 98.35\% \tag{4}$$

(iv) Percentage computational time improvement from Sai et al. [21] is

$$= \left(\frac{53.85 - 1.44}{53.85}\right) * 100 = 97.32\% \tag{5}$$

Table 4: Communication overhead analysis of the designed framework with relevant schemes.

Ref. no.	Ciphertext size
Saeed et al. [18]	$\lvert m\rvert + 5\lvert G\rvert = 5632\ bits$
Iqbal et al. [19]	$\lvert m\rvert + 5\lvert G\rvert = 5632\ bits$
Ashibani and Mahmoud [20]	$\lvert m\rvert + 2\lvert G\rvert = 2560\ bits$
Sai et al. [21]	$\lvert m\rvert + 4\lvert G\rvert = 4608\ bits$
Designed framework	$\lvert m\rvert + 3\lvert N\rvert = 752\ bits$

6.2. Communication Overhead. In this section, we compare the proposed framework with some relevant online/offline signcryption approaches cited [18–21] in terms of communication overhead with the including parameters bilinear pairing and Hyperelliptic Curve Cryptosystem. The bits size of the given parameters is taken from [24, 25].

(i) Bits utilized by Bilinear Pairing $(G) = 1024$

(ii) Bits utilized by Hyperelliptic Curve Cryptosystem $(N) = 80$

(iii) Bits utilized by plaintext $(m) = 512$

Table 4 shows the communication overhead of the aforementioned parameters in the proposed framework and the relevant online/offline signcryption schemes cited [18–21]. Lastly, Figure 4 clearly demonstrates the efficiency of the proposed framework in terms of communication overhead.

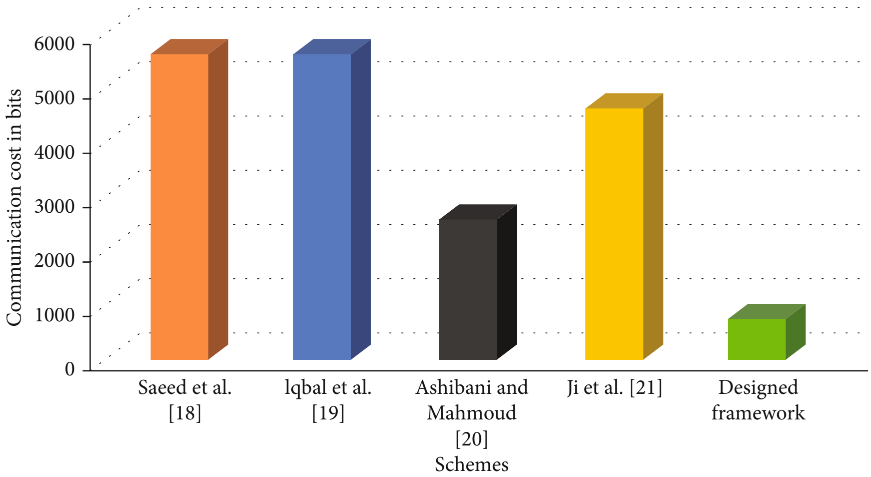


Figure 4: Communication cost analysis.

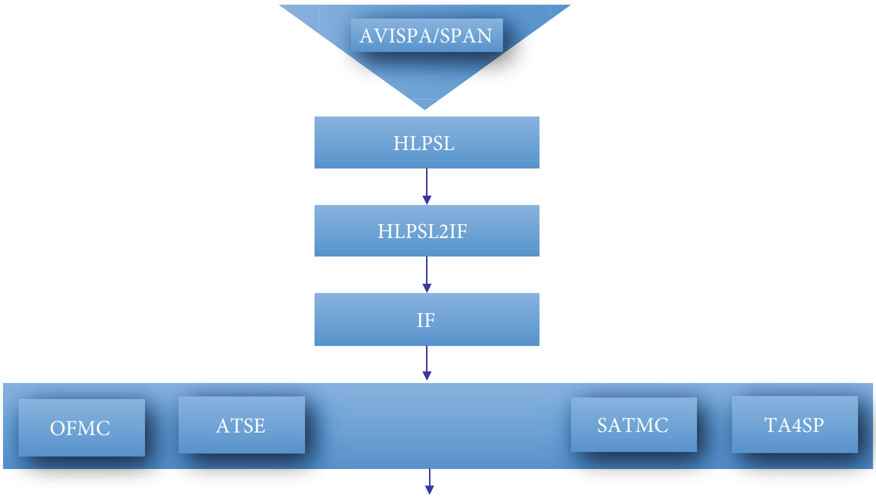


Figure 5: Top-down flow of AVISP

6.2.1. Percentage Improvement. The percentage of communication overhead improvement can be calculated using the given formula:

$$\left(\frac{\textit{Cost of previous scheme} - \textit{Cost of proposed scheme}}{\textit{Cost of previous scheme}}\right) * 100. \tag{6}$$

(i) Percentage communication overhead improvement from Saeed et al. [18] is

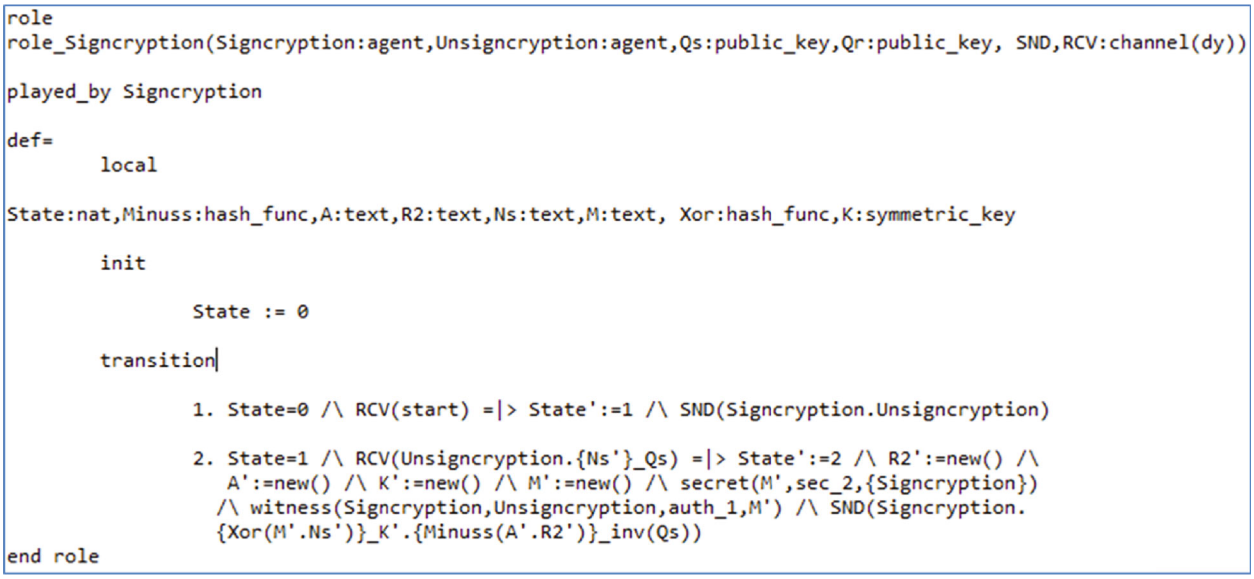
$$= \left(\frac{5632 - 752}{5632}\right) * 100 = 86.64\% \tag{7}$$

(ii) Percentage communication overhead improvement from Iqbal et al. [19] is

$$= \left(\frac{5632 - 752}{5632}\right) * 100 = 86.64\% \tag{8}$$

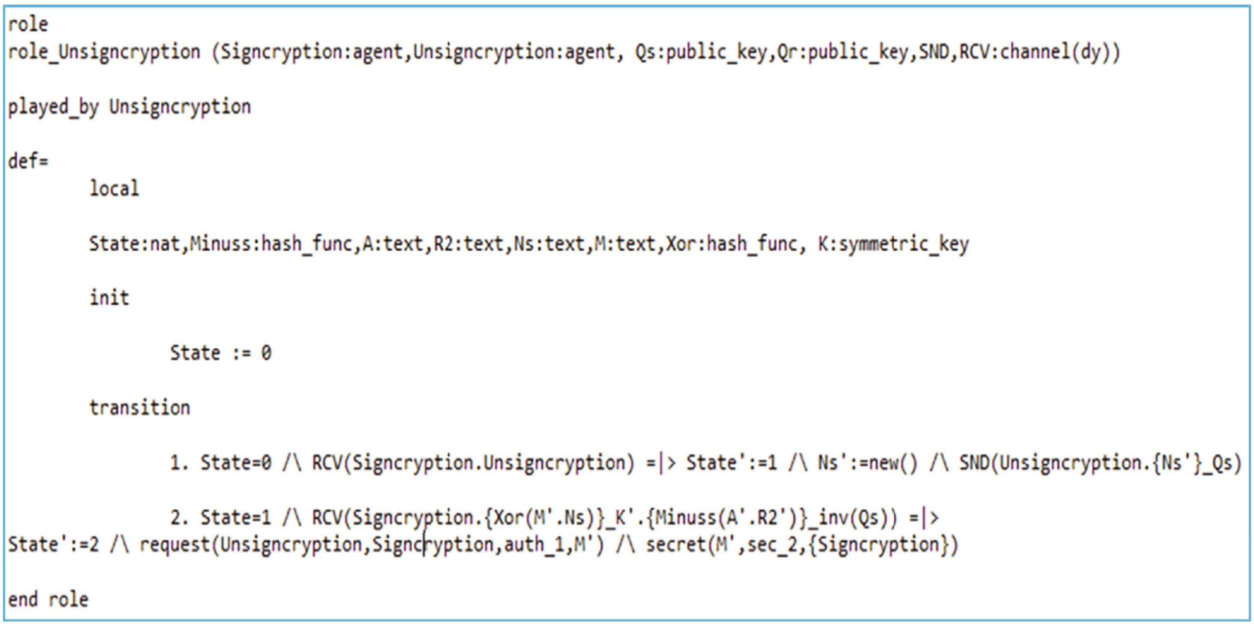
(iii) Percentage communication overhead improvement from Ashibani and Mahmoud et al. [20] is

$$= \left(\frac{2560 - 752}{2560}\right) * 100 = 70.62\% \tag{9}$$



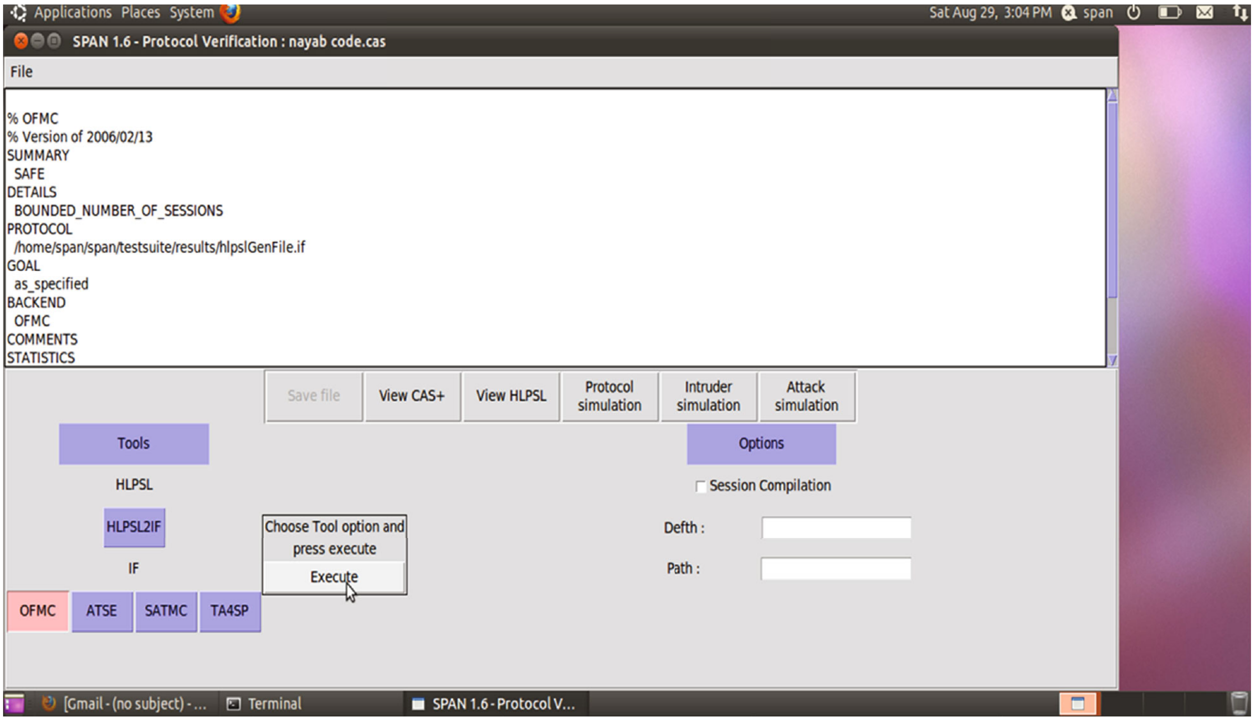
```
role
role_Signcryption(Signcryption:agent,Unsigncryption:agent,Qs:public_key,Qr:public_key, SND,RCV:channel(dy))

played_by Signcryption

def=
        local

State:nat,Minuss:hash_func,A:text,R2:text,Ns:text,M:text, Xor:hash_func,K:symmetric_key

        init

                State := 0

        transition

                1. State=0 /\ RCV(start) =|> State':=1 /\ SND(Signcryption.Unsigncryption)

                2. State=1 /\ RCV(Unsigncryption.{Ns'}_Qs) =|> State':=2 /\ R2':=new() /\
                   A':=new() /\ K':=new() /\ M':=new() /\ secret(M',sec_2,{Signcryption})
                  /\ witness(Signcryption,Unsigncryption,auth_1,M') /\ SND(Signcryption.
                  {Xor(M'.Ns')}_K'.{Minuss(A'.R2')}_inv(Qs))
end role
```

Figure 6: HLPSL code of signcryption.



```
role
role_Unsigncryption (Signcryption:agent,Unsigncryption:agent, Qs:public_key,Qr:public_key,SND,RCV:channel(dy))

played_by Unsigncryption

def=
        local

        State:nat,Minuss:hash_func,A:text,R2:text,Ns:text,M:text,Xor:hash_func, K:symmetric_key

        init

                State := 0

        transition

                1. State=0 /\ RCV(Signcryption.Unsigncryption) =|> State':=1 /\ Ns':=new() /\ SND(Unsigncryption.{Ns'}_Qs)

                2. State=1 /\ RCV(Signcryption.{Xor(M'.Ns)}_K'.{Minuss(A'.R2')}_inv(Qs)) =|>
State':=2 /\ request(Unsigncryption,Signcryption,auth_1,M') /\ secret(M',sec_2,{Signcryption})

end role
```

Figure 7: HLSL code for un-signcryption.



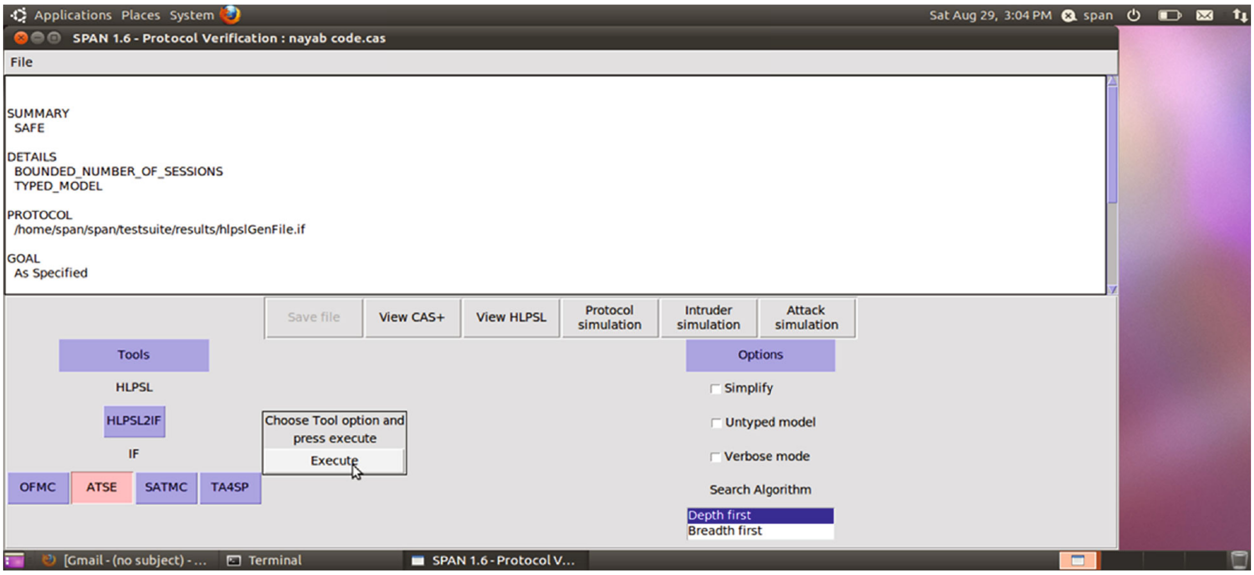
```
% OFMC
% Version of 2006/02/13
SUMMARY
 SAFE
DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
 /home/span/span/testsuite/results/hlpslGenFile.if
GOAL
 as_specified
BACKEND
 OFMC
COMMENTS
STATISTICS
```

☐ Session Compilation

Defth :

Path :

Figure 8: Simulation result of OFMC.



```
SUMMARY
 SAFE

DETAILS
 BOUNDED_NUMBER_OF_SESSIONS
 TYPED_MODEL

PROTOCOL
 /home/span/span/testsuite/results/hlpslGenFile.if

GOAL
 As Specified
```

☐ Simplify

☐ Untyped model

☐ Verbose mode

Search Algorithm

Depth first

Breadth first

Figure 9: Simulation result of AtSe.

(iv) Percentage communication overhead improvement from Sai et al. [19] is

$$= \left(\frac{4608-752}{4608}\right) * 100 = 83.68\% \qquad (10)$$

7. Conclusion

In this paper, we proposed an online/offline signcryption approach for IoT-enabled smart homes in a certificateless environment. The proposed approach is based on the Hyperelliptic Curve Cryptosystem (HCC), a lightweight complexity algorithm that is well-suited to resource-constrained smart home devices. According to security analysis, the designed framework meets the security requirements of integrity, unforgeability, secrecy, anti-replay attack, and non-repudiation. The proposed scheme's efficiency and effectiveness are demonstrated by the complexity analysis of computation and communication costs. Finally, we used the AVISPA tool to verify our proposed framework. The output findings show that the framework is secure against malicious threats.

Appendix

A.1. AVISPA

We used the well-known validation tool "AVISPA" to test the security of the designed framework. The AVISPA tool [26] is used to ensure the security of cryptographic protocols that have been built. To show the security to be validated, an HLPSL [27] is used. As shown in Figure 5, the CAS+ specification [28] gives an input to Security Protocol ANimator (SPAN), which converts it to HLPSL script. It is in charge of analyzing the conversion using the AVISPA. To ensure that the objectives set out in the target section of the HLPSL are met, the AVISPA tool uses four backend tools: Satisfaction-based Model-Checker (SATMC), On-the-Fly Model-Checker (OFMC), Auto Approach-based Tree Automata security protocol analysis (TA4SP), and Control-Logic-Based Attack Search (CLAtSe). It uses a series of repeated procedures to test the backend protocol until it is confirmed to be safe or until some vulnerabilities are detected from time to time. HLPSL creates a model of the process based on the sessions. Because a lot of variables change during each session, the status can change.

A.2. AVISPA Validation Results

Using AVISPA, we provide validation findings for the proposed framework. First, we generate the HLPSL code for our proposed algorithm. After that, we run the code via the AVISPA tool's embedded backends, OFMC and ATSE. As shown in Figures 6 and 7, the designed scheme is tested hundreds of times to create a secure output under the backbends. We used a Haier Intel Core i3-4010U processor with 1.70 GHz and 4 GB of RAM, as well as Windows 8.1 software. In addition, on Ubuntu 10.10 light 1, we used Oracle Virtual Box (V.5.2.0.118431). As demonstrated in Figures 6 and 7, the HLPSL code has two major roles: role signcryption and role unsigncryption. Figures 8 and 9 also show that the suggested framework is safe when used with the AVISPA backends OFMC and ATSE.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgments

This research was supported by the Researchers Supporting Project number (RSP2022R476), King Saud University, Riyadh, Saudi Arabia.

References

[1] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, pp. 909–920, 2020.

[2] J. Iqbal, M. Adnan, Y. Khan et al., "Designing a healthcare-enabled software-defined wireless body area network architecture for secure medical data and efficient diagnosis," *Journal of Healthcare Engineering*, vol. 2022, Article ID 9210761, 19 pages, 2022.

[3] A. Asif, E. Savas, H. AlSalman, M. Arshad, A. Gumaei, and A. Rehman, "Fixed point of rational contractions and its application for secure dynamic routing in wireless sensor networks," *Security and Communication Networks*, vol. 2021, 10 pages, 2021.

[4] K. Peterson, D. Sloo, Y. Matsuoka, and N. U. Webb, "Smart-home system facilitating insight into detected carbon monoxide levels," U.S. Patent 10, 546, 469, 2020.

[5] A. Gumaei, M. Al-Rakhami, M. M. Hassan et al., "A deep learning-based driver distraction identification framework over edge cloud," *Neural Computing and Applications*, pp. 1–16, 2020.

[6] H. Li, K. Yu, B. Liu, C. Feng, Z. Qin, and G. Srivastava, "An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things," *IEEE Journal of Biomedical and Health Informatics*, 2021.

[7] M. Pau, E. Patti, L. Barbierato et al., "A cloud-based smart metering infrastructure for distribution grid services and automation," *Sustainable Energy, Grids and Networks*, vol. 15, pp. 14–25, 2018.

[8] C. Meshram, A. Alsanad, J. V. Tembhurne et al., "A provably secure lightweight subtree-based short signature scheme with fuzzy user data sharing for human-centered IoT," *IEEE Access*, vol. 9, pp. 3649–3659, 2021.

[9] M. Kumar, H. K. Verma, and G. Sikka, "A secure lightweight signature based authentication for Cloud-IoT crowdsensing environments," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 4, article e3292, 2019.

[10] S. Rajesh, V. Paul, V. G. Menon, and M. R. Khosravi, "A secure and efficient lightweight symmetric encryption scheme for transfer of text files between embedded IoT devices," *Symmetry*, vol. 11, no. 2, p. 293, 2019.

[11] S. Mandal, B. Bera, A. K. Sutrala, A. K. Das, K. K. R. Choo, and Y. Park, "Certificateless-signcryption-based three-factor user access control scheme for IoT environment," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3184–3197, 2020.

[12] A. Karati, C. I. Fan, and R. H. Hsu, "Provably secure and generalized signcryption with public verifiability for secure data transmission between resource-constrained IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10431–10440, 2019.

[13] M. Luo, M. Tu, and J. Xu, "A security communication model based on certificateless online/offline signcryption for Internet of Things," *Security and Communication Networks*, vol. 7, no. 10, 1569 pages, 2014.

[14] W. Shi, N. Kumar, P. Gong, N. Chilamkurti, and H. Chang, "On the security of a certificateless online/offline signcryption for Internet of Things," *Peer-to-Peer Networking and Applications*, vol. 8, no. 5, pp. 881–885, 2015.

[15] J. Li, J. Zhao, and Y. Zhang, "Certificateless online/offline signcryption scheme," *Security and Communication Networks*, vol. 8, no. 11, 1990 pages, 2015.

[16] F. Li, Y. Han, and C. Jin, "Certificateless online/offline signcryption for the Internet of Things," *Wireless Networks*, vol. 23, no. 1, pp. 145–158, 2017.

[17] Y. S. Rao, "Attribute-based online/offline signcryption scheme," *International Journal of Communication Systems*, vol. 30, no. 16, article e3322, 2017.

[18] M. E. S. Saeed, Q. Liu, G. Tian, B. Gao, and F. Li, "HOOSC: heterogeneous online/offline signcryption for the Internet of Things," *Wireless Networks*, vol. 24, no. 8, pp. 3141–3160, 2018.

[19] J. Iqbal, A. I. Umar, N. Amin, and A. Waheed, "Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain," *International Journal of Distributed Sensor Networks*, vol. 15, no. 9, 2019.

[20] Y. Ashibani and Q. H. Mahmoud, "An efficient and secure scheme for smart home communication using identity-based signcryption," in *2017 IEEE 36th International Performance Computing and Communications Conference (IPCCC)*IEEE.

[21] S. Ji, R. Huang, J. Shen, X. Jin, and Y. Cho, "A certificateless signcryption scheme for smart home networks," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 7, p. 1, 2021.

[22] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on information theory*, vol. 29, no. 2, pp. 198–208, 1983.

[23] M. Rehman, H. Khattak, A. S. Alzahrani et al., "A lightweight nature heterogeneous generalized signcryption (hgsc) scheme for named data networking-enabled internet of things," *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8857272, 20 pages, 2020.

[24] S. S. Ullah, I. Ullah, H. Khattak et al., "A lightweight identity-based signature scheme for mitigation of content poisoning attack in named data networking with Internet of Things," *IEEE Access*, vol. 8, pp. 98910–98928, 2020.

[25] S. Hussain, I. Ullah, H. Khattak et al., "A lightweight and formally secure certificate based signcryption with proxy re-encryption (CBSRE) for Internet of Things enabled smart grid," *IEEE Access*, vol. 8, pp. 93230–93248, 2020.

[26] AVISPA, *Automated Validation of Internet Security Protocols and Applications*, 2017, http://www.avispa-project.org/.

[27] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, and L. Compagna, Eds.J. Cuéllar, P. H. Drielsma, P. C. Héam, O. Kouchnarenko, J. Mantovani, and S. Mödersheim, "the AVISPA tool for the automated validation of internet security protocols and applications," in *International conference on computer aided verification*, pp. 281–285, 2005.

[28] R. Saillard and T. Genet, "CAS+," 2018, Available at http://people.irisa.fr/Thomas.Genet/span/CAS_manual.pdf.