An Efficient and Secure Scheme for Smart Home Communication using Identity-Based Signcryption

Yosef Ashibani, Qusay H. Mahmoud
Department of Electrical, Computer and Software Engineering
University of Ontario Institute of Technology
Oshawa, Ontario, L1H 7K4 Canada
{yosef.ashibani,qusay.mahmoud}@uoit.net

***Abstract*—Securing communication between users and devices is an important aspect of Internet of Things applications. Although a number of cryptographic schemes have been proposed for securing communication among IoT devices, the ability to handle such schemes, especially with devices that have constrained computing resources, is difficult. Thus, there is a need for a secure and efficient scheme that will protect connections between devices with limited capabilities. For overcoming such constraints, many symmetric and asymmetric cryptographic techniques have been proposed. However, not all of the available cryptographic mechanisms can satisfy all of the security goals. Fortunately, there is a single mechanism that can provide combined security goals with low cost in terms of computation and communication overhead in addition to memory requirement. This technique, known as signcryption, can more efficiently satisfy authentication, integrity and confidentiality than combining encryption and signature schemes. This paper presents an identity-based signcryption scheme for smart home communication. Analysis and evaluation show that, in addition to efficiently providing authentication, the proposed scheme provides integrity and confidentiality as well as the ability to protect communication between devices against possible attacks.**

Keywords: Security, Authentication, IoT, Smart Home, Signcryption

I. Introduction

The Internet of Things (IoT) has applications in many domains such as smart home, where baby monitor cameras, garage door locks and smart lighting can be remotely accessed and controlled. Most of the interconnections are achieved wirelessly via the Internet for reasons such as availability and cost effectiveness in providing remote access and control as well as convenience to users [1]. However, the number of connected devices results in security vulnerabilities. Attacks against such devices, which often have limited capabilities and are usually connected through the Internet by commonly using less secure wireless media, might easily achieve access to sensitive data. This emphasizes the importance of authenticity, which should be ranked first since it is the most important part of security and that on which other security classes are built [2]. While satisfying authentication mostly depends on cryptographic techniques, not all devices with limited capabilities can perform the required computation capabilities.

An important issue is the secure transmission of user information between IoT devices. For example, if a transmitted message contains private information, such as application usage logs and sensor data, is exploited by an adversary, it will threaten the data integrity, thus affecting the privacy of the user. Hence, transferring any information that can be utilized for characterizing users' behavior must be protected from disclosure. One important aspect of security regarding data transmission is device-to-device message authentication. However, the majority of home devices are designed to consume low power with small size hardware, resulting in constrained computing performance with limited memory storage [3]. Thus, there is a need for designing a scheme that is capable of efficiently achieving the appropriate security requirements. It is also recognized that not all available cryptographic mechanisms satisfy all the security goals. Fortunately, there is a single mechanism that can provide combined security goals with lower cost in terms of computation and communication in addition to memory requirement. This process, known as signcryption, can satisfy message authentication, integrity and confidentiality more efficiently than combining encryption and signature schemes [4] [5], which in turn enables the adoption of this mechanism by smart home devices. Many signcryption schemes have been proposed based on ElGamal and RSA. Nevertheless, not all of them can efficiently meet all security goals.

A suitable cryptographic technique is identity-based cryptography (IBC), which could solve the security issues in device communication for smart homes. Shamir was the first to mention the idea of the identity-based signature scheme in 1984. Although Shamir was able to construct this scheme based on the RSA algorithm, he was not able to construct an IBE scheme. This problem was not resolved until 2001 when Boneh and Franklin were able to extend the concept of identity-based to develop schemes for encryption and decryption based on pairing on elliptic curves [6].

978-1-5090-6468-7/17/$31.00 ©2017 IEEE

A. Motivation

IoT security has been the primary concern of most users as well as one of the most important reasons for determining the adoption of IoT applications, such as smart homes. Many smart home devices, such as baby monitor cameras, garage door locks and smart lighting, can be controlled through end-user devices such as a smartphone or a tablet. Smart home applications connect, for example, many devices and objects to one another, and the interconnection of these devices to the end-user device can be achieved wirelessly and through the Internet, thus making users' daily life easier. However, these devices may contain personal information related to the users. Thus, insecure communication from one device to another may lead to private information disclosure which in turn could be targeted by attackers. An effective solution that secures communication among these devices is the cryptographic technique. However, not all cryptographic mechanisms can be applied efficiently to those devices with constrained computation capabilities. Hence, there is a need for a lightweight security scheme that achieves all the security goals while considering the resource limitations of such devices.

Many lightweight security schemes have been proposed based on symmetric key cryptography. These schemes need a number of shared symmetric keys for each party. If the shared key is compromised, all the communicated messages will be compromised. For providing higher security, public key cryptography has been used. However, public key cryptography still needs a certificate for each public key, which is considered a complex process. Any new proposed security scheme should satisfy the following requirements: any proposed cryptographic solution should be computationally less intensive to be able to run on devices with limited capabilities; any involved devices should be able to authenticate any transmitted message, without involving a third party in each transaction, and have the ability to protect against possible attacks. These requirements can be met by adopting identity-based cryptography for securing communication among devices in smart homes that have limited resources. IBC uses short encryption keys and is considered stronger than other cryptographic techniques regarding computation and efficiency [1]. A signcryption technique based on the IBC can more efficiently satisfy both signature and encryption than individually combining encryption and signature schemes [4]. To this end, the contributions of this paper are:

- A signcryption scheme based on IBC that provides authentication for smart home communication.
- The proposed scheme does not require access to a trusted third party during the authentication process, and this access is only needed at the registration time or for updating secret keys.
- In addition to providing authentication, the proposed scheme provides integrity and confidentiality as well as the ability to protect communication among devices against various possible attacks.
- The proposed scheme is more efficient regarding cipher-text length and computational cost compared to other existing signcryption schemes.

The rest of this paper is organized into the following sections. Section II provides a summary of relevant related work. Section III presents the system model and design goals. Bilinear pairing, complexity assumptions and identity-based signcryption are presented in Section IV while the proposed scheme is described in Section V. Performance evaluation and security analysis are introduced in Sections VI and VII, respectively. Finally, Section VIII provides the conclusion and suggestions for future research directions.

II. Related Work

In recent years, many schemes have been proposed for securing communication either intended or that could be adopted for smart homes. In general, many available devices in the market are provided with the ability to securely communicate by utilizing a 128-bit basic hashing cryptography scheme. For communication between any two devices, a pre-shared symmetric key should be exchanged in advance for encrypting and decrypting any transmitted messages. This approach requires a regular key exchange among devices. If the used key is compromised, all communicated messages will be compromised [7]. For example, authors in [8] [9] present a lightweight cryptographic technique for resource-constrained devices by combining symmetric and asymmetric cryptography in addition to hash functions, providing confidentiality, integrity, authentication and non-repudiation. However, the proposed technique mainly depends on symmetric cryptography for data encryption.

A lightweight encryption scheme for smart homes that provides confidentiality with less overhead in computation and communication is presented in [10]. This scheme adopts IBE, which requires minimal public key management, and the authors also provide a security analysis showing the efficiency of the proposed scheme. However, the focus of the proposed scheme is mainly on confidentiality. Moreover, it is based on symmetric cryptography for message encryption, which weakens the security of the proposed scheme. A common symmetric key that is automatically generated according to extracted parameters from wireless multi-path channels is presented in [11]. This approach is mainly intended for devices that support 802.11a protocol. A radio frequency for consumer electronics secure key pairing protocol is proposed in [12]. For authentication, the proposed scheme requires each device to communicate with its manufacturer. In this technique, each involved device is required to send authentication information to its manufacturer through a mobile operator in order to be authenticated. This scheme is based on symmetric key cryptography, and there is always a need for access to the device's manufacturer in order to be authenticated and this could be difficult.

A security scheme that provides three levels of authentications among gateway, smart meter, smart appliances and the home area network is proposed in [13]. However, the provided scheme mainly depends on a third party (e.g., the Internet service provider) for providing three security levels. A secure smart household appliance framework has been proposed in [14]. The focus of this framework is on providing safe operations, smart home safety and electricity price control. For reliable security protection, this framework employs machine learning but does not account for device authentication, integrity and data confidentiality, which are the main security goals. A key establishment protocol for smart homes is presented in [15]. This protocol is based on elliptic curve cryptography and requires a trusted certificate authority for providing public and private keys. Although the authors provide a limited security analysis, it needs to be emphasized that involving traditional public key cryptography requires a third party for certification and, in turn, this produces more overhead on constrained devices. The authors in [16] propose a lightweight mutual message authentication scheme for reducing the number of exchanged messages during authentication. Although the proposed scheme provides two-step mutual authentication, it uses public key encryption combined with Diffie-Hellman key exchange schemes.

Although there are many proposed public cryptographic mechanisms, not all of them efficiently satisfy all the security goals. A suitable cryptographic technique that could solve the security issues in device communication for smart homes is the IBC based on elliptic curve cryptography, which outperforms other public key cryptography, such as RSA [17], in terms of key size and cryptographic operations. To the best of our knowledge, no signcryption scheme has been proposed for securing smart home communications, which is the primary focus of this paper.

III. System Model and Design Goals

This section presents the system model, attack model and security requirements of the proposed scheme.

A. System Model

In this paper, we consider a smart home system model, as shown in Figure 1, which consists of four main parties: a number of home devices; an end-user device; a home gateway; and a trusted local server. The end-user device, which could be any smart device such as a smartphone or a tablet, is used as a node in our smart home model. Furthermore, we consider the communication process as any message exchanged between any home device and end-user device.

- Home Devices: Home devices are any devices (e.g., surveillance camera, media server, smart lock, thermostat, refrigerator, or baby monitor) that can be remotely accessed. Some home devices, which communicate locally over wireless channels through the local home gateway, are resource constrained with limited computational capabilities, bandwidth and battery power.
- End-User Devices: End-user devices are any devices (e.g., smartphone or tablet) that can be used to access home devices. End-user devices are used to monitor and control home devices either locally through the WiFi or the Internet.
- Home Gateway (*HG*): The Home Gateway is a network entity that acts as an intermediary between home devices and end-user devices. The primary role of the HG is to help in exchanging messages locally among devices through either the WiFi or the Internet.
- Local Server (*LS*): We integrate a trusted local server that is responsible for initializing the system, registering new devices and assigning required secret communication parameters. The *LS* contains a database that records all the registered devices and the access log history.

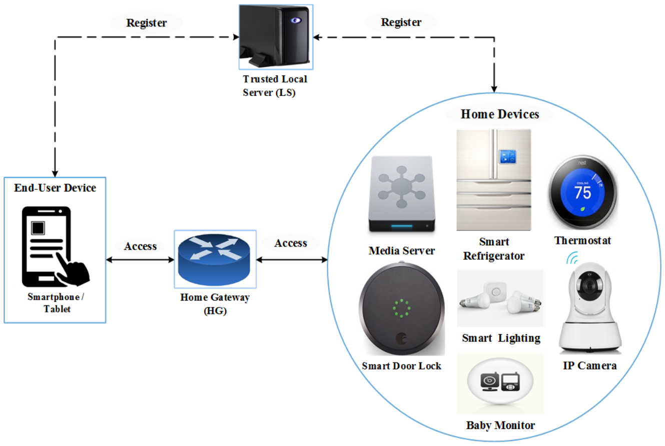

Figure 1: Smart home system architecture

B. Attack Model

In the attack model, we consider the HG as semi-trusted and the local server and end-user devices as trusted. Thus, if a transmitted message contains private information, it could be exploited by an adversary residing in the HG that could threaten data integrity and disclose user information. The following scenarios are examples of possible attacks:

- An adversary may masquerade as another entity and gain sensitive information from home devices to attack other home network components. For example, being able to launch a spoofing attack to obtain unauthorized access to monitor and control home devices such as a thermostat could lead to undesired consequences, which is a concern to homeowners. Therefore, message authentication should be performed by each entity involved in a smart home network to verify the source of any issued message.

- An adversary residing in HG might launch an active attack to target data integrity, such as modifying or altering a command during its transmission. For instance, an attacker could discover a command that is intended to close a door lock and change this command to open the door lock. Thus, the integrity of the transmitted messages must be satisfied.
- An adversary might also, as a result of being able to eavesdrop on a message transmission, discover a command message. For example, if able to reach a message command sent to a remote control door system to open or close a home door, an adversary would know whether the user is at home, which could result in the home being broken into, impacting confidentiality. Thus, any important information involved in the transmitted messages among devices must not be accessible to unauthorized parties.

C. *Design Goals*

Based on the attack model presented in the attack model subsection, from the initial connection of devices in a smart home, the following security requirements should be satisfied in order to prevent attacks:

- Authentication: Authentication should take place for any transmitted message to verify its source. The system can then prevent any unauthorized access to devices.
- Integrity: Integrity ensures that a transmitted message is not altered or generated by an attacker during its transmission.
- Confidentiality: Confidentiality should be satisfied to protect any disclosure of the transmitted messages among devices which may contain sensitive information that could be exploited by an adversary. Protecting any disclosure of the information related to home devices would also prevent users' private information being revealed.
- The proposed scheme should be lightweight, meaning lower cost in regard to computation and communication overhead.

IV. Preliminaries

This section presents some preliminaries that are used in this paper, and Table I shows the used notation throughout the paper.

A. *Bilinear Pairing*

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of order p for some large prime p, and $P_1 \in \mathbb{G}_1$ be the generator of $\mathbb{G}_1$. The IBE makes use of a bilinear pairing map $\hat{e} : \mathbb{G}_1 \text{ x } \mathbb{G}_1 \rightarrow \mathbb{G}_2$ between these two cyclic groups. The map must satisfy the following properties [18]:

- *Bilinear*: $\hat{e}(aP_1, bQ) = \hat{e}(P_1, Q)^{ab}$ for all P_1,$Q \in \mathbb{G}_1$ and all a, $b \in Z_p^*$.
- *Nondegenerate*: If P_1 is a generator of $\mathbb{G}_1$, then $\hat{e}(P_1, P_1)$ is a generator of $\mathbb{G}_2$, thus $\hat{e}(P_1, P_1) \neq 1$.
- *Computable*: There is an efficient algorithm to compute $\hat{e}(P_1, Q)$ for all P_1,$Q \in \mathbb{G}_1$.

A bilinear map that satisfies the aforementioned properties above is said to be an *admissible* bilinear pairing map $\hat{e} : \mathbb{G}_1 \text{ x } \mathbb{G}_1 \rightarrow \mathbb{G}_2$. The Weil pairing or Tate pairing can be used to construct an admissible bilinear map between these two groups over elliptic curves [18].

B. *Complexity Assumptions*

The proposed scheme is based on two Diffie-Hellman problems as follows:

- *Assumption* 1: (Computational Diffie-Hellman problem (CDH)). Given the elements $(P_1, aP_1, bP_1) \in \mathbb{G}_1$ for unknown a, $b \in Z_p^*$, there is no polynomial time to compute $abP_1 \in \mathbb{G}_1$.
- *Assumption* 2: (Bilinear Diffie-Hellman problem (BDH)). Given the elements $(P_1, aP_1, bP_1, cP_1) \in \mathbb{G}_1$ for unknown $a, b, c \in Z_p^*$, it is difficult to compute $\hat{e}(P_1, P_1)^{abc} \in \mathbb{G}_1$.

Table I: Defeinitions of the used notations

Notation	**Definition**
LS	trusted local server
HG	Home Gateway
ID_{LS}	unique identity of the LS
Q_{LS}	public identity of the LS
S_{LS}	private identity of the LS
ID_{di}	unique identity of a device i
Q_{di}	public identity of a device i
S_{di}	private key of a device i
k	security parameter
s	secret master key of the LS
p	k bit prime number
$\hat{e}$	admissible bilinear parameter
H_1 , H_2	secure cryptographic hash functions
Z_p^*	set of elements $\{0, ..., p-1\}$
P_1	the generator of $\mathbb{G}_1$
$\mathbb{G}_1$	a subgroup of additive group of points
$\mathbb{G}_2$	a subgroup of multiplicative group of points
r_i	a random integer $r_i \in Z_p^*$
m	(message) plaintext
n	plaintext lenght
C	cipher-text
σ	the signcrypted message
m'	the unsigncrypted message

C. Identity-Based Signcryption

Identity-Based Signcryption (IBS) includes four steps: system initialization, registration, signcryption and unsigncryption. The function of each step is outlined below.

- System initialization: The LS uses a security parameter k to generate the public system parameters while keeping k parameter secret.
- Registration and public key generation: Given an identity of a device ID_{di}, the LS computes the corresponding private key S_{di} and sends it back to the device.
- Signcryption: To send a message m to a receiver with identity ID_{di}, the sender encrypts the message m and then signs it consecutively using the public parameters resulting from the system initialization stage including S_{di} of the sender and ID_{di} of the receiver, and the message m producing a cipher-text σ.
- Unsigncryption: When the receiver receives the cipher-text σ from the sender device, it unsigncrypts it (using the sender's ID_{di}, the receiver's S_{di} and the cipher-text σ) to obtain the corresponding plaintext m after checking the correctness of the sender.

V. Proposed Scheme

This section presents the proposed scheme and the correctness of the retrieved message.

A. Scheme Details

The IBS includes four steps: system initialization, registration, signcryption and unsigncryption. These steps are described below.

1) System Initialization

In this stage, a trusted local server LS is responsible for configuring system parameters. In particular, using the security parameter k as input, the LS generates the bilinear parameters (p, P_1, $\mathbb{G}_1$, $\mathbb{G}_2$, $\hat{e}$) by running $g$en(k), and chooses two secure cryptographic hash functions: H_1 :$\{0,\ 1\}^* \rightarrow \mathbb{G}_1$ and H_2 : $\mathbb{G}_2 \rightarrow \{0,\ 1\}^n$ (n : *plain text lenght*). The LS chooses a random number $s \in Z_p^*$ which is kept as a master secret, and then calculates $P_{pub} = sP_1$. The *public parameters* $(p, P_1, \mathbb{G}_1, \mathbb{G}_2, n, \hat{e}, H_1, H_2, P_{pub})$ are then published by the LS.

2) Registration Stage

At this stage, as shown in Figure 2, each device submits its chosen identity ID_{di} to the LS, as depicted in step 1, which in turn generates the public identity Q_{di}, calculates the private key S_{di} using the master secret key s and sends them with the public parameters to the registered devices as depicted in step 2. For the first device, the LS calculates $Q_{d1} = H_1(ID_{d1})$ and $S_{d1} = s(Q_{d1})$, then sends the public identity and the private key to this device over a secure channel. Similarly, the second device sends the chosen identity (ID_{d2}) to the LS and consecutively receives the public identity $Q_{d2} = H_1(ID_{d2})$ and the private key $S_{d2} = s(Q_{d2})$. The LS's identity is $Q_{LS} = H_1(ID_{LS})$ and the private key is $S_{LS} = s(Q_{LS})$. After the registration stage, there is no need to communicate with the LS during the authentication process of any transmitted messages, as depicted in step 3. Access to the LS is only required at the time of registration or for updating secret keys.

3) Signcryption

We assume that the sender device is d_1 and the receiver device is d_2. Thus, the sender device now has the following parameters: (S_{d1}, Q_{d2}, m). In order to signcrypt a message $m \in \{0,1\}^n$, the proposed signcryption technique works as follows: it encrypts the message and then signs it consecutively using the *public parameters* resulting from the initialization stage as well as (S_{d1}, ID_{d2}, m). The actions of the sender device are described below.

Generates a random integer $r_i \in Z_p^*$ and then calculates the following:

$C_1 = r_i P_1$; Q_{d1} & Q_{d2} are already initialized in the registration stage.

$K = H_2(\hat{e}(r_i Q_{d2}, P_{pub}))$

$C_{enc} = (m \oplus K)$ is the cipher-text.

h= $H_1(C_{enc})$

$C_{sign} = r_i h + S_{d1}$, where S_{d1} is the sender's private key.

Result $\sigma = (C_1, C_{enc}, C_{sign})$ is the signcrypted message m by the sender device S_{d1}. The σ is then sent to the targeted receiver, device d_2.

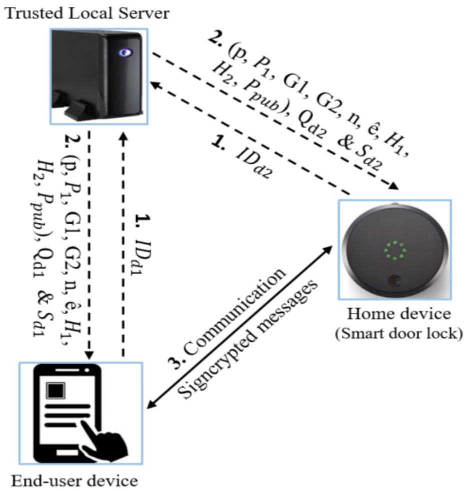
Trusted Local Server
2. (p, P_1, G1, G2, n, ê, H_1, H_2, P_{pub}), Q_{d2} & S_{d2}
1. ID_{d2}
2. (p, P_1, G1, G2, n, ê, H_1, H_2, P_{pub}), Q_{d1} & S_{d1}
1. ID_{d1}
Home device
(Smart door lock)
3. Communication
Signcrypted messages
End-user device

Figure 2: Operations of the proposed scheme

4) Unsigncryption

After receiving the signcryption message, d_2 first verifies the received message by running the following equations:

$$\hat{e}(P_1, C_{sign}) = \hat{e}(h, C_1)\ \hat{e}(Q_{d1}, P_{pub}) \tag{3.1}$$

If the equation (3.1) holds, it goes to the next step which is the unsigncryption, meaning that the received message m is authenticated. The unsigncryption algorithm works as follows:

Calculates $K' = H_2(\hat{e}(S_{d2}, C_1))$
Calculates $m' = C_{enc} \oplus K'$
Otherwise, it is invalid and the message will be rejected.

B. Correctness

The correctness of the retrieved message is achieved as follows:

- Correctness of Keys:

$$\begin{aligned} K' &= H_2(\hat{e}(sQ_{d2}, C_1)) \\ &= H_2(\hat{e}(sQ_{d2}, r_iP_1)) \\ &= H_2(\hat{e}(r_iQ_{d2}, sP_1)) \\ &= H_2(\hat{e}(r_iQ_{d2}, P_{pub})) \\ &= K \end{aligned}$$

- Correctness of equation (3.1):

$$\begin{aligned} \hat{e}(C_{sign}, P_1) &= \hat{e}(r_ih + sQ_{d1}, P_1) \\ &= \hat{e}(r_ih, P_1)\ \hat{e}(sQ_{d1}, P_1) \\ &= \hat{e}(h, r_iP_1)\ \hat{e}(sQ_{d1}, sP_1) \\ &= \hat{e}(h, C_1)\ \hat{e}(Q_{d1}, P_{pub}) \end{aligned}$$

- Correctness of Decryption:

$$\begin{aligned} m' &= C_{enc} \oplus K' \\ &= m \oplus k \oplus K' \\ &= m \end{aligned}$$

VI. Performance Evaluation

This section provides an evaluation of the proposed scheme regarding computation time and cipher-text length. For the evaluation purpose, the scheme is assessed according to the computation time that is taken by both the *Signcryption* and the *Unsigncryption* processes. For this evaluation, we consider the implementation of Tate pairing on an MNT curve with an embedding degree of $k = 6$ where $\mathbb{G}_1$ is represented by 161 bits, and order p represented by 160 bits on a machine with Intel Pentium IV 3.0 GHZ. Since pairing and point multiplication computations are the main computations in the proposed scheme, they have been considered in calculating the execution time in comparison with the related work. We adopt the measured processing time given in [19] [20] as follows: T_{mul}=0.6(ms) is the the time of a one point multiplication operation whereas $T_{\hat{e}}$=4.5(ms) is the time of a pairing operation in $\mathbb{G}_1$. As it can be seen in Table II, in the proposed scheme in this paper, there are three multiplication operations and five pairing operations for the whole scheme. In the signcryption stage there are three multiplication operations and one pairing operation, and in the unsigncryption stage there are four pairing operations. Thus, the time of signcryption and unsigncryption of the proposed scheme are calculated according to the following formula:

T_{total} (ms) = (number of the pairing operations) x $T_{\hat{e}}$ + (number of the multiplication operations) x T_{mul}

Thus, the execution time of the whole scheme will be: $T_{total} = 5$ x $T_{\hat{e}} + 3$ x $T_{mul} = 5$ x $4.5 + 3$ x $0.6 = 24.3\ ms$

Although we could not identify any signcryption scheme that is designed mainly for providing authentication in smart home communication, we evaluated our scheme by comparing it with two other IBS schemes given in [21] [22]. Table II provides a comparison of our scheme with these two schemes regarding the involved computations and total execution time. As can be seen from the results, the cipher-text length of our scheme and the presented scheme in [21] are similar. However, our scheme outperforms in relation to computational costs, requiring less computational time by 1.2 ms. Also, our scheme outperforms the scheme presented in [22] regarding both computational costs and cipher-text length. As shown in the comparison, our scheme requires less computational time by 0.6 ms, and cipher-text length. Thus, our scheme outperforms the other two schemes in the area of computational cost and cipher-text size.

Table II: Computational overhead and cipher-text length

Scheme	**Performed operations**			**Cipher-text Length**
	T_{mul}	$\hat{e}$	$T_{total}(ms)$	
This paper	3	5	24.3	$\lvert m\rvert + 2\lvert G\rvert$
[21]	5	5	25.5	$\lvert m\rvert + 2\lvert G\rvert$
[22]	4	5	24.9	$\lvert m\rvert + 2\lvert G\rvert + \lvert Z_p^*\rvert$

VII. Security Analysis

In this section, we analyze the security properties of the proposed scheme. The analysis focuses on how the proposed scheme can realize security requirements for smart home device communications.

1) Authentication: Only the messages signcrypted by a legitimate sender device with ID_{d1} could be unsigncrypted by the intended receiver with the corresponding ID_{d2}. Furthermore, only the local trusted server can compute the correct private key of the communicated devices. Thus, the proposed scheme can guarantee the message authentication among the end-user device and the home device as well as with the LS since this server is the only one that generates the public parameters and issues the private keys of the involved devices. Additionally, any messages cannot be signed by an adversary without having the sender's secret key S_{d1}.

2) Integrity: Based on the complexity assumptions outlined in section IV, which are provably secure in the random oracle model [18], any intercepted message by an attacker cannot be encrypted without reaching the randomly chosen number $r_i \in Z_p^*$ which is used for each message to be sent. A different random number is included in each new message and in the case of knowing this number, the future sent message will not use the same number, hence will resist against reply attack. As a result, the proposed scheme can protect against active attacks to target data integrity, such as modifying or altering a command during its transmission, thus protecting the integrity of any transmitted messages.
3) Confidentiality: As the private keys are generated and issued by the LS which is trusted, and these keys are transferred offline over a secure channel, an attacker cannot access the private keys of the connected devices. Since an attacker cannot decrypt the transmitted message without knowing the receiver's private key, message confidentiality is ensured.

VIII. Conclusion and Future Work

This paper provides an efficient and secure scheme for smart home communication using IBC which provides message source authentication. The presented scheme is based on securing communication between an end-user device and any home device. During the authentication process, the proposed scheme does not require access to a third party, and access to this party is only needed at the time of registration or for updating secret keys. In addition to providing authentication, the proposed scheme provides integrity and confidentiality as well as the ability to protect communication among devices against various possible attacks. Moreover, the proposed scheme achieves anonymity regarding device identity. Compared to other schemes, the proposed scheme can efficiently achieve the security requirements for device-to-device communication in the smart home. The local server that is responsible for parameter initialization and key generations is assumed to be secure. However, in the case of being attacked, all the issued secret keys can be realized. In order to solve this security issue, the direction of future work will be to investigate how to protect the local server in situations where it joins in the communication process. Future work will further include implementing the proposed scheme on real IoT devices and evaluating the performance in a real-world environment.

References

[1] Y. Ashibani and Q. H. Mahmoud, "Cyber physical systems security: analysis, challenges and solutions," *Computers & Security*, 2017.

[2] Y. Ashibani, D. Kauling, and Q. H. Mahmoud, "A context-aware authentication framework for smart homes," in *Electrical and Computer Engineering (CCECE), 2017 IEEE 30th Canadian Conference on.* IEEE, 2017, pp. 1–5.

[3] C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in *Communications and Network Security (CNS), 2014 IEEE Conference on.* IEEE, 2014, pp. 67–72.

[4] J. Malone-Lee, "Identity-based signcryption." *IACR Cryptology ePrint Archive*, vol. 2002, p. 98, 2002.

[5] K. Alharbi and X. Lin, "Efficient and privacy-preserving smart grid downlink communication using identity based signcryption," in *Global Communications Conference (GLOBECOM), 2016 IEEE.* IEEE, 2016, pp. 1–6.

[6] H. Phaneendra, "Identity-based cryptography and comparison with traditional public key encryption: A survey," *International Journal of Computer Science & Information Technology*, vol. 5, no. 4, p. 5521, 2014.

[7] D. M. Dobkin and B. Aboussouan, "Low power wi-fi$^{\text{TM}}$(ieee802. 11) for ipsmart objects," *GainSpan Corporation*, 2009.

[8] T. Bhattasali, "Licrypt: Lightweight cryptography technique for securing smart objects in internet of things environment," *CSI Communications*, 2013.

[9] J. Ayuso, L. Marin, A. Jara, and A. F. G. Skarmeta, "Optimization of public key cryptography (rsa and ecc) for 16-bits devices based on 6lowpan," in *1st International Workshop on the Security of the Internet of Things, Tokyo, Japan*, 2010.

[10] S. Al Salami, J. Baek, K. Salah, and E. Damiani, "Lightweight encryption for smart home," in *Availability, Reliability and Security (ARES), 2016 11th International Conference on.* IEEE, 2016, pp. 382–388.

[11] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking.* ACM, 2008, pp. 128–139.

[12] K. Han, J. Kim, T. Shon, and D. Ko, "A novel secure key paring protocol for rf4ce ubiquitous smart home systems," *Personal and ubiquitous computing*, vol. 17, no. 5, pp. 945–949, 2013.

[13] E. Ayday and S. Rajagopal, "Secure device authentication mechanisms for the smart grid-enabled home area networks," Tech. Rep., 2013.

[14] Y. Chen and B. Luo, "S2a: secure smart household appliances," in *Proceedings of the second ACM conference on Data and Application Security and Privacy.* ACM, 2012, pp. 217–228.

[15] Y. Li, "Design of a key establishment protocol for smart home energy management system," in *Computational Intelligence, Communication Systems and Networks (CICSyN), 2013 Fifth International Conference on.* IEEE, 2013, pp. 88–93.

[16] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. S. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 675–685, 2011.

[17] K. Magons, "Applications and benefits of elliptic curve cryptography." in *SOFSEM (Student Research Forum Papers/Posters)*, 2016, pp. 32–42.

[18] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM journal on computing*, vol. 32, no. 3, pp. 586–615, 2003.

[19] T. W. Chim, S.-M. Yiu, L. C. Hui, and V. O. Li, "Vspn: Vanet-based secure and privacy-preserving navigation," *IEEE Transactions on Computers*, vol. 63, no. 2, pp. 510–524, 2014.

[20] Y. Sun, R. Lu, and X. Lin, "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, 2010.

[21] B. Adiga, P. Balamuralidhar, M. Rajan, R. Shastry, and V. Shivraj, "An identity based encryption using elliptic curve cryptography for secure m2m communication," in *Proceedings of the First International Conference on Security of Internet of Things.* ACM, 2012, pp. 68–74.

[22] H. K.-H. So, S. H. Kwok, E. Y. Lam, and K.-S. Lui, "Zero-configuration identity-based signcryption scheme for smart grid," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on.* IEEE, 2010, pp. 321–326.