Lightweight Encryption for Smart Home

Sanaah Al Salami*, Joonsang Baek, Khaled Salah, Ernesto Damiani
Information Security Research Center
Khalifa University
Abu Dhabi, UAE
*Email: *sanaah.alsalami@kustar.ac.ae*

***Abstract*—Smart home is one of the most popular IoT (Internet of Things) applications, which connects a wide variety of objects and home appliances in a single logical network. Smart home applications have benefited from interactions and data transmissions among different devices over the integrated network with or without human interventions. However, like other technologies, smart home likely introduces new security vulnerabilities due to its dynamic and open nature of connectivity with heterogeneous features. Among such vulnerabilities, is the breach of confidentiality which needs to be addressed urgently as data exchanged between smart home devices can contain crucial information related to user's privacy and safety. However, some of the challenges in providing smart home system with confidentiality service are the flexibility of key management and efficiency of computation and communication. These challenges should be addressed carefully as many small and resource-constrained devices are usually involved in smart home systems. In this paper, we address these challenges by proposing a lightweight encryption scheme for smart homes. This scheme will provide users and smart objects with confidentiality service without incurring much overhead cost associated with computation and communication. Our proposed scheme also supports flexible public key management through adopting identity-based encryption, which does not require complex certificate handling. We provide a formal security analysis of our scheme and a performance simulation study. The simulation shows that our scheme provides favorable level of efficiency in terms of overhead cost associated with computation and communication.**

***Keywords*-Smart Home; Internet of Things; Security; Identity-Based Encryption; Lightweight Encryption; IoT**

I. Introduction

A. Motivation

Smart home system is becoming gaining popularity as it provides a controlled and monitored system in a home environment where exchange of information among smart devices and sensors are readily available. As illustrated in Figure 1, in smart home system, all home appliances such as climate control, smart alarm, surveillance cameras, curtains, home entertainment system, access control, door control and many more can be controlled through a user's smart phone or other devices connected to the Internet.

With smart home being an emerging technology of the Internet of Things (IoT), which connects all the aforementioned home appliances and objects one another, and integrate them to the Internet through smartphones and other mobile devices, our daily life is becoming smarter and easier. However, all those connected devices may contain personal data flowing from one device to another.

Figure 1. Smart Home Concept

Also it may be that simple but sensitive information, for example, whether or not the main door is open, can be exchanged without being protected. Indeed, in terms of smart home system, it is natural for anyone to be worried about his/her personal data being leaked especially from a home because home is considered as sanctuary where no one wants it to be controlled by intruders or attackers. (This may be the reason why Mattern and Floerkemeier wrote that the Internet of Things (IoT) realizes "old dream" or "nightmare" of smart home [14].) Moreover, there are a great deal of data transactions that occur in smart home systems especially when they are connected to the Internet 24/7. As we are all aware, the Internet has been targeted often by adversaries who want to steal information as much as possible.

One of the obvious ways to break the privacy of data in smart home is breaking into the weakest device or using infected device that can compromise the whole network by opening the door to attackers who can retrieve all the information they want from the device or even gain control over the other devices. By doing so, they will be able to compromise the whole smart home system eventually [10][11][12][13]. Whether data is on the move or at rest, the risk remains high where smart home users need to be

978-1-5090-0990-9/16 $31.00 © 2016 IEEE
DOI 10.1109/ARES.2016.40

assured that in all cases, their data is safe and protected [12][16].

For this reason, it is important to protect smart home system by means of cryptography. Nevertheless, providing security through cryptography is not always easy: Efficiency needs to be almost always attained as many smart home objects and appliances are resource-constrained. Hence it might be necessary to implement a lightweight cryptographic solutions, so-called "lightweight cryptography (LWC)" to save computations, communications, storage and eventually power consumption. But a problem here is that almost all the available LWC is based on symmetric key cryptography, requiring users to share a number of symmetric keys to each of smart home devices. This can be troublesome if not impossible. To resolve this issue, we may consider to use public key cryptography but another problem is that we need digital certificate for each public key to ensure its authenticity. As is well known, managing public key infrastructure is complex and it is hard to imagine that all the smart home devices have public keys that come with digital certificates. In this paper, we deal with these issues.

B. Related Work

There have been a few studies in the field of smart home security, most of which focus on the security challenges that vendors and implementers face when adopting a smart home concept and how to address those challenges. Some vendors proposed various architectures and frameworks of smart home to secure smart home devices while others recommended combinations of technologies to enhance the security of devices and to ensure data protection. Furthermore, there were papers that discussed common security challenges of smart home in terms of IoT, such as privacy, authentication, inter-compatibility and secure end-to-end connection. The most common recommendation is to secure all OSI seven layers which will strengthen the security and minimize the risk of compromising a device or an object in the smart home network [11].

Jiang et al. [10] explained a wide variety of network technologies in smart home focusing on three main areas which are "Powerline", "Busline"and "Radio frequency". Powerline consist of wired devices connected to the main power supply by the same power supply cables, and considered the cheapest and fastest to build. In case of any malfunctions or failures, it requires physical support in the house to fix it. The main issue related to this technology is that it suffers from interferences and power cuts that might cause the system to fail. On the other hand, Busline uses different cables than the power supply to connect the devices and transmit data, and considered the most reliable technology for smart home because it prevents device failure during the power cuts. Radio frequency is becoming more popular in smart home, but suffers from issues such as interferences, device short-range issues and security issues where intruders can gain access to the devices and the home by modifying the settings [10].

Han et al.[9] and Santoso et al. [16] investigated diverse components that need to be included in any smart home systems where each component has a specific role. They discussed "home gateway", whose main purpose is to integrate different technologies, standards and IoT devices and to provide access from home to external services. In addition, the user can use home gateway to connect his/her smartphone in order to access the smart home system from the outside and control the different devices in the home network while smart home devices provide the information flowing between all devices and the internet.

Other works by Lee et al.[11] and Yuan et al. [17] also treated security problems in smart home as those in general IoT which provide an interaction between different smart objects with access to the Internet through using different network technologies such as ZigBee, Wi-Fi and Bluetooth with the help of network gateways. Such works focused on analyzing the security threats and challenges in smart home implementation where there is a need to secure the physical layer, information and communication between devices by using a safe mechanism called Terminal-Gateway-Group system. Note that terminal is the mobile terminal, gateway refers to a home gateway, and group refers to sensor nodes. The cooperation between sensor layer, network layer and application layer will ensure home automation in a safe way. This will ensure confidentiality, completeness and authenticity. The foundation for this mechanism is the usage of ZigBee wireless network, Internet, GSM and the CC2530 hardware platform.

Furthermore, Bhattasali [4] and Ayuso et al. [1] suggested that lightweight cryptographic technique can be used for resource constrained devices which consume low power and hence has limited bandwidth. This technique will combine three different cryptographic primitives such as symmetric cryptography, asymmetric cryptography and hash functions. The usage of these algorithms will provide confidentiality, integrity, authentication and non-repudiation. Implementing them can be either software-oriented or hardware-oriented. Most of the hardware-oriented security algorithms are actually implemented by the vendors who are providing the smart devices in IoT. Choosing the right cryptographic algorithm is always based on the requirements that take the first priority with respect to the constraints a smart object have as well as the cost. Although it seems nearly impossible to implement asymmetric cryptography in constrained objects, elliptic curve cryptography (ECC) made that possible due to its structure and small key sizes which require small memory and computations.

However, to our knowledge, cryptographic solutions based on a variety of primitives including identity-based encryption and stateful public key encryption have not been applied to smart home security, which will be a main focus of this paper.

C. Our Contributions

In this paper, we address the confidentiality issue of smart home applications. Our contributions can be sum-

marized as follows.

1) We propose a lightweight encryption scheme for smart homes, called "LES (lightweight encryption for smart homes)". This scheme is identity-based, meaning the public keys used for this scheme are merely identity strings, which do not need certificate. The identity-based property turns out to be useful in managing encryption keys for smart home devices. This scheme is also "stateful" [3] meaning some part of cryptographic computations are repeated across sessions, which is to boost computational efficiency. In order to provide efficiency in communications, our scheme separates key encryption and data encryption in such a way that key encryption is less frequently performed.
2) We provide a security definition for LES and analyze the security of the proposed LES scheme based on the definition provided. Our analysis shows that our scheme provides indistinguishable encryption agains chosen plaintext attack (i.e. IND-CPA secure) in the random oracle model assuming that the bilinear Diffie-Hellman (BDH) problem [5][6][2] is hard.
3) We present simulation results based on our implementation of the proposed LES scheme to conduct performance analysis. It shows that our LES scheme provides high level of efficiency required for smart home applications in terms of computation and communication compared with the previous schemes in the literature without optimizations.

The rest of this paper is organized as follows. Section II presents cryptographic methodologies, protocols and concepts that the proposed scheme will employ. Section III describes the proposed LES scheme. This section also discusses one of the scenarios as to how the LES scheme can be used for the smart home application. Section IV presents security and performance analysis of the proposed scheme. Section V concludes the paper.

II. Preliminaries

In this section, we review various cryptographic primitives that our proposed LES scheme will use.

The first primitive is identity-based encryption (IBE) [5][6][2]. As illustrated in Figure 2, IBE uses identities represented by strings such as IP or email addresses or possibly MAC address as a public key for data encryption. The private key generator (PKG) will issue private keys which are associated with those identities. By removing dependency on the public key infrastructure (PKI), IBE reduces system complexity and cost as digital certificates for public keys are no longer needed. The downside of IBE, however, is that it is computationally expensive [2] compared with other regular public key schemes as most likely it needs a special function called "pairing" which turns out to be a few times more expensive than a single exponentiation.

Many researches have focused on providing efficiency for public key cryptographic algorithms by employing optimization technique such as reducing the number of

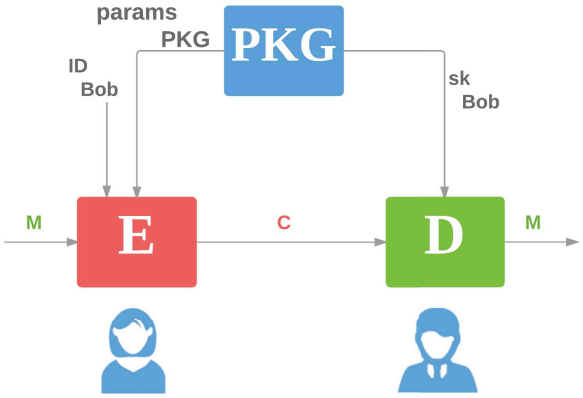

Figure 2. Identity-Based Encryption

discrete exponentiations. The optimization is important for pubic key cryptographic schemes and protocols to be implemented on resource-constrained devices. One notable technique in this line of research is to make a public key encryption algorithm "stateful" in such a way that some (expensive) parts of encryption operation such as exponentiation are reused across multiple encryptions to save computation [3]. Decryption will remain the same. This technique turns out to be useful to reduce computational overhead, compared with the standard stateless public key encryption algorithms.

Phong, Matsuoka and Ogata (PMO) considered how to combine IBE and stateful public key encryption [15]. They proposed a stateful version of Boneh and Franklin's IBE scheme [5]. We are particularly interested in this scheme as it will provide a useful tool for securing communications in smart home applications. However, we realized that this scheme can be further optimized by separating key encryption, which produces relatively long ciphertexts, from data encryption, which usually produces short ciphertexts in smart home applications.

III. Our Scheme

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your system, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

In this section, we provide a description of our scheme, which we call "Lightweight Encryption for Smart Home (LES)".

Our scheme is based on Phong, Matsuoka and Ogata (PMO)'s stateful IBE (IBE) [15] scheme, which combines identity-based encryption [5] and stateful Diffie-Hellman (DH) encryption scheme [3] as mentioned in the previous section. Note that the stateful DH scheme reduces computing exponentiations in the DH-based encryption by making use of *state* to gain efficiency, in other words, randomness reuse to save computation. This can informally be described as follows: In the stateful DH scheme, the ephemeral exponent of DH key (g^r, y^r), where $y = g^x$,

r can be reused by saving r in the state. (That's why the encryption is called to be stateful.) Although this may weaken the security of encryption, it can be alleviated by using a stronger symmetric encryption algorithm, which provides inexpensive yet fast random encryption.

Note also that in smart home applications, not only reducing computational complexity, but also reducing communication cost is important. In order to address this issue, we make our scheme to have two-sub algorithms, called "KEYEncrypt" and "DATAEncrypt". The former algorithm is to encrypt a session key while the latter is to encrypt messages under the chosen key. This is reminiscent of KEM/DEM (Key Encapsulation Mechanism/ Data Encapsulation Mechanism) framework of hybrid encryption [7] but a difference is that in our LES scheme, we transmit a ciphertext resulted from KEYEncrypt, which we call a "key ciphertext" and a ciphertext resulted from DATAEncrypt, which we call a "data ciphertext" *separately*. In other words, a ciphertext that encrypts a current session key can be transmitted once while ciphertexts generated under this session key can be transmitted multiple times (without attaching the key cipertext). Indeed, in the setting of the stateful encryption, it would not be necessary to send key ciphertexts, whose major parts are repetitive due to stateful nature of the scheme and by not doing so would save significant communication cost. However, the remaining question is whether allowing it results in a secure (at lest against chosen plaintext attack) encryption scheme. The answer is positive: Later, we show that as long as a symmetric encryption scheme that is used to implement DATAEncrypt is secure against chosen plaintext attack, the whole LES scheme is also secure.

A. *The Proposed* LES *Scheme*

As follows is the details of our LES scheme based on pairing, which we denote by LES.

- Setup: The base station (BS), acting as the private key generator (PKG) in IBE [5], [6], generates $\mathbb{G}_1$ and $\mathbb{G}_2$, both of which have the same prime order q, and selects an admissible pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, where g is a generator of $\mathbb{G}_1$. It then picks $s \in \mathbb{Z}_q$ at random and computes $y = g^s$. The BS also selects a symmetric encryption scheme (E, D), where E and D denote encryption and decryption procedures respectively. The BS also chooses two hash functions $\mathsf{H}_1 : \{0,1\}^* \to \mathbb{G}_1$ and H_2: $\mathbb{G}_2 \to \{0,1\}^n$ for some positive integer n, which is the size of the key. (That is, $\{0,1\}^n$ is key space.) The BS sets secret master key $mk = s$ and a set of public parameters $params = (\mathbb{G}_1, \mathbb{G}_2, e, g, y, (\mathsf{E}, \mathsf{D}), \mathsf{H}_1, \mathsf{H}_2)$. The BS distributes $params$ to all of the entities involved.
- Extract: Upon receiving an identity $\mathtt{ID}$, the BS computes $\mathsf{H}_1(\mathtt{ID})^s \in \mathbb{G}_1$ and returns $K_{\mathtt{ID}} = \mathsf{H}_1(\mathtt{ID})^s$ as a private key associated with $\mathtt{ID}$.
- KEYEncrypt: The sender performs the following.
  - Pick a symmetric key k uniformly at random from the key space $\{0,1\}^n$.
  - If $st = \mathtt{NULL}$, do the following:
    - Pick $r \in \mathbb{Z}_q$ uniformly at random.
    - Compute $u = g^r$ and $v = \mathsf{H}_2(e(\mathsf{H}_1(\mathtt{ID}), y)^r) \oplus k$.
    - Set $st = (r, g^r, e(\mathsf{H}_1(\mathtt{ID}), y)^r)$.
  - Else do the following:
    - Parse st as $(r, g^r, e(\mathsf{H}_1(\mathtt{ID}), y)^r)$.
    - Set $u = g^r$ and compute $v = \mathsf{H}_2(e(\mathsf{H}_1(\mathtt{ID}), y)^r) \oplus k$.
  - Return $C_k = (u, v, \mathtt{ID})$ as "key ciphertext".
- DATAEncrypt: Search the random symmetric key k that corresponds to $\mathtt{ID}$. Then perform the following.
  - Compute $C_m = \mathsf{E}_k(m)$.
  - Return C_m as "data ciphertext".
- KEYDecrypt: Upon receiving key ciphertext $C_k = (u, v, \mathtt{ID})$, the receiver performs the following using $K_{\mathtt{ID}}$.
  - Compute $k = v \oplus \mathsf{H}_2(e(K_{\mathtt{ID}}, u))$.
  - Return k.
- DATADecrypt: Upon receiving data ciphertext C_m, the receiver finds k, which corresponds to $\mathtt{ID}$, performs the following using k, the decrypted symmetric key.
  - Compute $m = \mathsf{D}_k(C_m)$.
  - Return m.

Note that the pairing e is assumed to be a symmetric pairing and should satisfy the following properties [6][5]: 1) Non-degeneracy: $e(g, g) \neq 1 \in \mathbb{G}_2$; 2) Bilinearity: For all $a, b \in \mathbb{Z}_q$, $e(g^a, g^b) = e(g, g)^{ab}$.

B. *Application to Smart Home*

As its name stands for, our LES scheme is designed to be used in smart home applications. It can be applied in the following scenario: Suppose that a user is trying to open the front door of his/her house remotely. In the house, a smart lock system is placed. The user will send a message to unlock the door through his/her smartphone. However, the message that commands the smart lock system to open the door contains sensitive information whether the door is currently locked or not. This information can be useful for a burglar who is trying to break into the house. For this reason, the message needs to be encrypted.

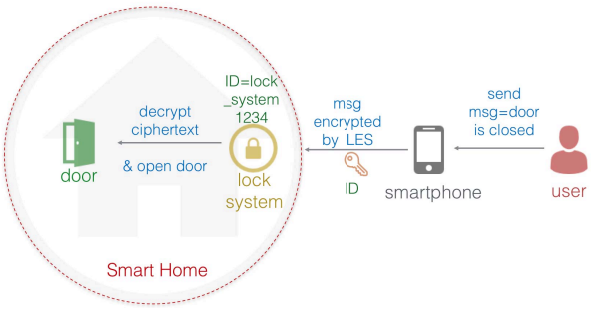

Figure 3. LES Application

IV. Analysis of our scheme

In this section, we present security and performance analysis of the proposed LES scheme.

A. Security Analysis

We first define the security of the LES scheme presented in the previous section. Basically, we require KEYEncrypt and DATAEncrypt schemes provide indistinguishable encryption under chosen plintext attack, i.e., they should be IND-CPA secure for the whole LES scheme to be IND-CPA secure. A formal definition is as follows.

Definition 1 (IND-CPA of LES): Let LES denote the lightweight encryption scheme for smart home. Consider the following game for adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, where $\mathcal{A}_1$ is a sub-attack algorithm for KeyEncrypt and $\mathcal{A}_2$ is a sub-attack algorithm for DataEncrypt with respect to security parameter λ.

As follows is $\mathbf{Game}^{\mathrm{IND-CPA}}_{\mathcal{A}_1,\mathsf{KEYEncrypt}}(\lambda)$, an attack game for $\mathcal{A}_1$:

1) Setup: The Setup algorithm is run with a security parameter λ to generate system parameters $params$ and master key mk. Then, $params$ is given to A_1, while mk is kept secret.
2) State Generation: The game runs the algorithm NwSt with input params to generate a state st, which will be used for encryption.
3) Phase 1: $\mathcal{A}_1$ adaptively makes the following queries:
   - Extraction query $\mathtt{ID}$: On receiving this query, the game runs the Extract algorithm to generate a private key $K_{\mathtt{ID}}$, and returns it to $\mathcal{A}_1$.
   - Key Encryption query $(\mathtt{ID}, k)$: On receiving this query, the game runs the KEYEncrypt algorithm to encrypt k using identity $\mathtt{ID}$ under the current state st. The resulting ciphertext C_k is given to $\mathcal{A}_1$.
4) Challenge: The adversary outputs a pair of equal-length keys (k_0, k_1) and an identity $\mathtt{ID}^*$ on which it wants to be challenged. Here, there is a restriction that $\mathtt{ID}^*$ was not issued as a private key extraction query in Phase 1. On receiving this, The game picks $\beta \in \{0, 1\}$ at random, computes $(C^*_{k_\beta}, st^*)$, where st^* is current state with respect to $\mathtt{ID}^*$, and only $C^*_{k_\beta}$ is returned to $\mathcal{A}_1$.
5) Phase 2: The adversary may adaptively makes more of the following queries:
   - Extraction query $\mathtt{ID}(\neq \mathtt{ID}^*)$: The game responds in the same way as done in Phase 1.
   - Key Encryption query $(\mathtt{ID}, k)$: The game responds in the same way as done in Phase 1.
6) Guess: Finally, $\mathcal{A}_1$ outputs a bit β' as its guess on β.

As follows is $\mathbf{Game}^{\mathrm{IND-CPA}}_{\mathcal{A}_2,\mathsf{DataEncrypt}}(\lambda)$, an attack game for A_2:

1) Phase 1: $\mathcal{A}_2$ adaptively makes a Data Encryption query m: On receiving this query, the game runs the DataEncrypt algorithm to encrypt m under the current key k. The resulting ciphertext C_m is given to $\mathcal{A}_2$.
2) Challenge: The adversary outputs a pair of equal-length mesages (m_0, m_1) on which it wants to be challenged. On receiving this, The game picks $b \in \{0, 1\}$ at random, computes C^*_m, which is returned to $\mathcal{A}_2$.
3) Phase 2: The adversary may adaptively makes more of Data Encryption query m: The game responds in the same way as done in Phase 1.
4) Guess: Finally, $\mathcal{A}_2$ outputs a bit b' as its guess of b.

We define that the LES scheme provides indistinguishable encryption against chosen plaintext attack, i.e., IND-CPA secure if KEYEncrypt and DATAEncrypt are IND-CPA secure. In other words, for all probabilistic polynomial-time adversaries $\mathcal{A}_1$ there is a negligible function $\varepsilon(\lambda)$ such that

$$\Pr[\mathbf{Game}^{\mathrm{IND-CPA}}_{\mathcal{A}_1,\mathsf{KEYEncrypt}}(\lambda) = 1] \leq \frac{1}{2} + \varepsilon(\lambda),$$

where the probability is taken over the randomness used by $\mathcal{A}_1$ and the randomness used in the game. Also, for all probabilistic polynomial-time adversaries $\mathcal{A}_2$, there is a negligible function $\varepsilon(\lambda)$ such that

$$\Pr[\mathbf{Game}^{\mathrm{IND-CPA}}_{\mathcal{A}_2,\mathsf{DATAEncrypt}}(\lambda) = 1] \leq \frac{1}{2} + \varepsilon(\lambda),$$

where the probability is taken over the randomness used by $\mathcal{A}_2$ and the randomness used in the game.

We now prove that our LES scheme is IND-CPA secure in the sense of Definition 1. More precisely, we prove the following lemma.

Lemma 1: Our LES scheme is IND-CPA secure assuming that the underlying KEYEncrypt is IND-ID-CPA secure in the random oracle model and the DATAEncrypt is IND-CPA secure.

Proof: We analyze the security of our protocol using a reduction argument. First, we show that the security of Phong, Matsuoka and Ogata (PMO)'s stateful IBE scheme is reduced to the security of KeyEncrypt in the sense of IND-ID-CPA. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be an adversary for our scheme, where $\mathcal{A}_1$ and $\mathcal{A}_2$ denote sub-attack algorithms for KeyEncrypt and DataEncrypt respectively. Let $\mathcal{B}$ be an adversary for the PMO scheme. $\mathcal{A}_1$ makes two types of queries, each of which is answered by $\mathcal{B}$ as follows:

- Hash query (random oracle query): On receiving this query, $\mathcal{B}$ simply forwards it to its random oracle H_1 or H_2 to get an answer and relays it to $\mathcal{A}_1$.
- Key extraction query $\mathtt{ID}$: On receiving this query, $\mathcal{B}$ simply forwards $\mathtt{ID}$ to its key extraction oracle to get an answer (a private key associated with ID) and relays it to $\mathcal{A}_1$.
- Challenge query (k_0, k_1), where $|k_0| = |k_1|$: On receiving this query, $\mathcal{B}$ simply forwards it to its encryption oracle as its challenge query to get an answer (a challenge ciphertext that encrypts one of k_0 and k_1, chosen at random, with a public part of state) and relays it to $\mathcal{A}_1$.

When $\mathcal{A}_1$ output its guess $\beta \in \{0,1\}$ on which of k_0 and k_1 has been encrypted, $\mathcal{B}$ outputs β as its answer. This is a prefect simulation. Hence, if the PMO scheme is IND-ID-CPA secure, which is the case KeyEncrypt is also IND-ID-CPA secure. (since IND-ID-CCA security of the PMO scheme implies that it is also IND-ID-CPA secure.) Note that the PMO scheme is based on the random oracle model.

Second, we show that DataEncrypt is also IND-CPA secure. This is also can be proven using a reduction argument. Using A_2 as a subroutine, an adversary $\mathcal{C}$ for *any* IND-CPA secure encryption can be constructed: Whenever $\mathcal{A}_2$ makes an encryption query, $\mathcal{C}$ forwards it to its encryption oracle to get a corresponding ciphertext and forwards it back to $\mathcal{A}_2$. When $\mathcal{A}_2$ makes a challenge query (m_0, m_1), where $|m_0| = |m_1|$, $\mathcal{C}$ forwards it to its encryption oracle as its challenge query to get an answer (a challenge ciphertext that encrypts one of m_0 and m_1, chosen at random) and relays it to $\mathcal{A}_2$. When $\mathcal{A}_2$ output its guess $b \in \{0,1\}$ on which of m_0 and m_1 has been encrypted, $\mathcal{C}$ outputs b as its answer. This is a perfect simulation. ■

Note that KeyEncrypt is IND-ID-CPA secure in the random oracle model assuming that the Bilinear Diffie-Hellman (BDH) problem is hard as proven by PMO [15]. The BDH problem refers to the computational problem to find $e(g,g)^{abc}$ given that g^a, g^b and g^c, where g is a generator of $\mathbb{G}_1$ and a, b and c are chosen at random from $\mathbb{Z}_q$. Thus, from Lemma 1, we obtain the following theorem.

Theorem 1: Our LES scheme is IND-CPA secure assuming that the BDH problem is hard in the random oracle model and the DATAEncrypt is IND-CPA secure.

We remark that all the IBE schemes have a drawback that the PKG is in possession of the master key can decrypt any ciphertexts. This issue requires the PKG to be an entity that is well trusted. This key escrowing property can serve for good purpose so that in case any user is suspected for a crime or any illegal activities, the PKG will use their power to decrypt the messages and confirm if allegations are true or not [2]. However, the key escrowing problem will not be a big issue in our LES scheme since the base station (BS) acting as the PKG can be part of the smart home system (not an external entity) where it acts as the server for all smart home appliances and devices and establish secure communications among them. Of course, the base station, which is connected to the Internet should be protected from intruders through any network security measures.

B. Performance Analysis

The main computational efficiency gain for the proposed LES scheme is from using the state, which is computed only once between a smart home device and a user per communication. Moreover, the usage of symmetric key encryption is fast and cheap, and hence it does not incur heavy computation for resource-constrained smart home devices.

To demonstrate the efficiency, we implemented our scheme on a Macintosh computer with a 1.1-GHz CPU and 8GB RAM using Java package for pairing computation, called "JPair" developed by Dong [8]. We used the Tate pairing defined over a supersingular curve with representation size of 512 bits in $\mathbb{G}_1$ is 512 bits as in Boneh and Frankiln's IBE scheme [5][6]. We used SHA1 for the hash function H_2, which is used as a key derivation function (KDF). The symmetric encryption was implemented using AES with CFB (Cipher Feedback) mode of operation.

We ran our scheme to simulate a scenario where a user communicates with a smart home device by exchanging a confidential message 10 to 50 times. We set up the identity as `ID = lock_system_1234` and encrypt the message M = `unlock the door`. We compared the running time of our LES scheme with that of the regular IBE, which is not stateful.

Table I summarizes the running time of regular IBE and LES in milliseconds.

No. of Encryptions	Regular IBE	LES
10	257.4707	24.3511
20	479.7013	59.4077
30	577.2992	66.9232
40	751.2355	75.2006
50	893.3837	80.4685

Table I
RUNNING TIME OF REGULAR IBE AND LES (OUR SCHEME) IN MILLISECONDS

In Figure 4, we illustrate the above running time. It is

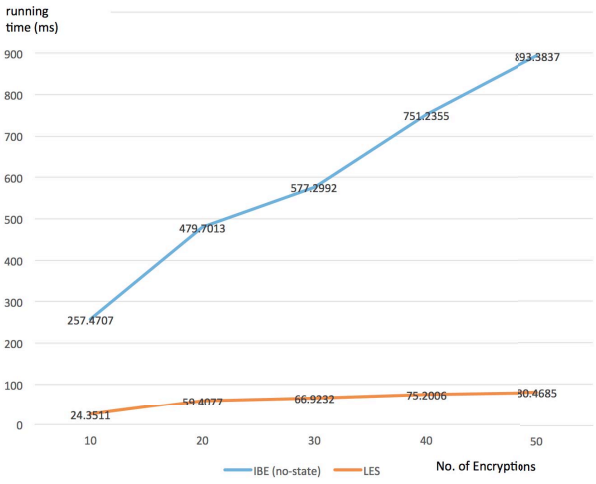

Figure 4. Illustration of Running time of regular IBE and LES

clear that the stateful property of encryption provides high compuational efficiency. Compared with stateless version of IBE, there is a dramatic speed-up (nearly 10 times) of encryption operations in our LES scheme.

We also measured communication overhead (the size of ciphertexts) of our scheme and compared it with that of regular IBE. As it can be seen from Table II, the separation of key and data encryption brings out good

communication efficiency. It reduces the communication overhead to approximately one-third.

No. of Encryptions	Regular IBE	LES
10	7360	2752
20	14720	4992
30	22080	7232
40	29440	9472
50	36800	11712

Table II
COMMUNICATION OVERHEAD OF REGULAR IBE AND LES (OUR SCHEME) IN BITS

V. CONCLUSION

In this paper, we proposed a Lightweight Encryption Scheme LES to be used for smart home applications. By employing the techniques of identity-based encryption and stateful encryption [15], our scheme provides flexibility in encryption key management and significant efficiency gains for encryption operation. Formal security analysis for the proposed scheme was presented in the paper.

Moreover, we implemented our scheme using Java language. The performance study of this implementation confirms the theoretically estimated efficiency of the proposed scheme. - It turns out that the stateful property of the encryption process significantly reduces the overall computational cost of encryption when multiple messages are encrypted.

In general, we envision that our LES scheme can be applied to not only smart home systems but also to other IoT-based systems. We hope that this study could be a small step forward for deploying identity-based cryptography to resource-constrained devices rather than depending only on less-functional symmetric key cryptography.

Our future research includes extending the implementation of our LES scheme to the various smart home devices on different platforms.

REFERENCES

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

[2] J. Baek, J. Newmarch, R. Safavi-Naini, and W. Susilo. A survey of identity-based cryptography. In *Proc. of Australian Unix Users Group Annual Conference*, pages 95–102, 2004.

[3] M. Bellare, T. Kohno, and V. Shoup. Stateful public-key cryptosystems: how to encrypt with one 160-bit exponentiation. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 380–389. ACM, 2006.

[4] T. Bhattasali. Licrypt: Lightweight cryptography technique for securing smart objects in internet of things environment.

[5] D. Boneh and M. Franklin. Identity based encryption from the weil pairing. *SIAM J. on Computing*, 32(3):586–515, 2003.

[6] X. Boyen. A tapestry of identity-based encryption: Practical frameworks compared. *International Journal of Applied Cryptography*, 1(1):3–21, 2008.

[7] R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM J. on Computing*, 33(1):167–226, 2003.

[8] C. Dong. Jpair: A quick introduction. Available at: https://personal.cis.strath.ac.uk/changyu.dong/jpair/intro.html.

[9] J.-H. Han, Y. Jeon, and J. Kim. Security considerations for secure and trustworthy smart home system in the iot environment. In *Information and Communication Technology Convergence (ICTC), 2015 International Conference on*, pages 1116–1118. IEEE, 2015.

[10] L. Jiang, D.-Y. Liu, B. Yang, et al. Smart home research. In *Proceedings of the Third Conference on Machine Learning and Cybernetics SHANGHAI*, pages 659–664, 2004.

[11] 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*, pages 67–72. IEEE, 2014.

[12] T. Mantoro, M. A. M. Adnan, and M. Ayu. Secured communication between mobile devices and smart home appliances. In *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference on*, pages 429–434. IEEE, 2013.

[13] T. Mantoro, M. Ayu, et al. Securing the authentication and message integrity for smart home using smart phone. In *Multimedia Computing and Systems (ICMCS), 2014 International Conference on*, pages 985–989. IEEE, 2014.

[14] F. Mattern and C. Floerkemeier. From the internet of computers to the internet of things. *From Active Data Management to Event-Based Systems and More*, pages 242–259, 2003.

[15] L. T. Phong, H. Matsuoka, and W. Ogata. Stateful identity-based encryption scheme: faster encryption and decryption. In *ASIACCS '08 Proceedings of the 2008 ACM symposium on Information, computer and communications security*, pages 381–388. ACM, 2008.

[16] F. K. Santoso and N. C. Vun. Securing iot for smart home system. In *Consumer Electronics (ISCE), 2015 IEEE International Symposium on*, pages 1–2. IEEE, 2015.

[17] X. Yuan and S. Peng. A research on secure smart home based on the internet of things. In *Information Science and Technology (ICIST), 2012 International Conference on*, pages 737–740. IEEE, 2012.