An Efficient Data Protection Scheme Based on Hierarchical ID-Based Encryption for MQTT

CHUN-I FAN, {Department of Computer Science and Engineering, Information Security Research Center, Intelligent Electronic Commerce Research Center}, National Sun Yat-sen University, Taiwan
CHENG-HAN SHIE, Department of Computer Science and Engineering, National Sun Yat-sen University, Taiwan
YI-FAN TSENG*, Department of Computer Science, National Chengchi University, Taiwan
HUI-CHUN HUANG, Department of Computer Science and Engineering, National Sun Yat-sen University, Taiwan

As Internet of Things (IoT) thriving over the whole world, more and more IoT devices and IoT-based protocols have been designed and proposed in order to meet people's needs. Among those protocols, message queueing telemetry transport (MQTT) is one of the most emerging and promising protocol, which provides many-to-many message transmission based on the "publish/subscribe" mechanism. It has been widely used in industries such as the energy industry, chemical engineering, self-driving, etc. While transporting important messages, MQTT specification recommends the use of TLS protocol. However, computation cost of TLS is too heavy. Since topics in a broker are stored with a hierarchical structure, In this manuscript, we propose a novel data protection protocol for MQTT from hierarchical ID-based encryption. Our protocol adopts the intrinsic hierarchical structures of MQTT, and achieves constant-size keys, i.e. independent of the depth in hierarchical structures. Besides, the formal security model for the proposed protocol have been defined in the manuscript. The proposed protocol have been formally proven chosen-plaintext secure under the ℓ-wBDHI assumption.

CCS Concepts: • **Computer systems organization** → *Sensor networks*; • **Security and privacy** → **Public key encryption**; • **Networks** → Network reliability.

Additional Key Words and Phrases: Hierarchical ID-Based Encryption, Message Queueing Telemetry Transport, MQTT, Data Protection.

ACM Reference Format:
Chun-I Fan, Cheng-Han Shie, Yi-Fan Tseng, and Hui-Chun Huang. 2018. An Efficient Data Protection Scheme Based on Hierarchical ID-Based Encryption for MQTT. In . ACM, New York, NY, USA, 21 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Internet of Things (IoT) has been used worldwide in the past decade. According to the report from Statista [16], the number of connected devices, not only for general customers but industries, will increase to around 25 billion in 2025, as shown in Figure 1. The term IoT generally refers to scenarios that are made up of things or devices connected by the Internet. They can interact with each other, absorb and share information. For IoT devices to communicate, a data protocol is required. As of now, there are several data protocols when it comes to connecting various devices in an IoT environment, such as CoAP [11] (Constrained Application Protocol), XMPP [10] (Extensible Messaging and Presence Protocol), MQTT [15] (Message Queueing Telemetry Transport) and so on. Among those protocols, MQTT is the first to be proposed and the most complete one. Besides, it is the only protocol that supports many-to-many transmissions

*The corresponding author

Manuscript submitted to ACM

(Figure 2). The introduction for MQTT is presented in Section 2.1.

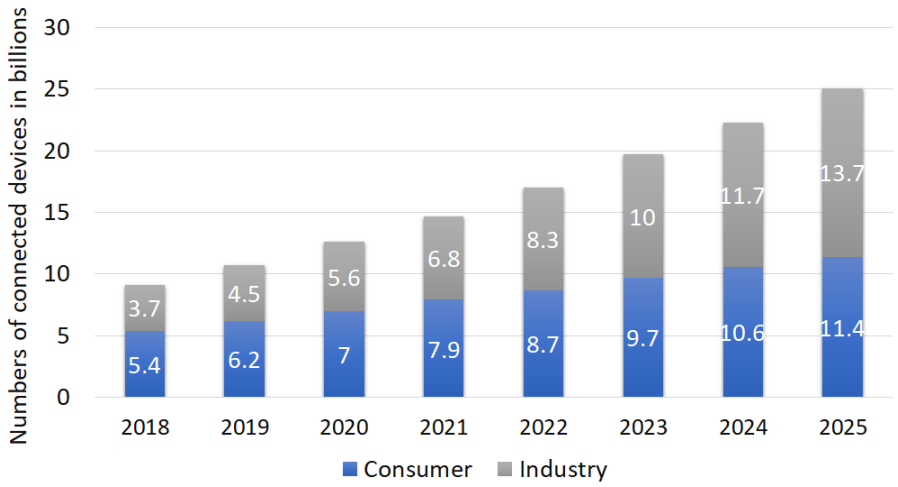

Fig. 1. Forecast numbers of Internet of Things (IoT) connected devices worldwide from 2018 to 2025 (in billions)

The concept of MQTT was first proposed by Andy Stanford-Clark and Arlen Nipper from IBM and Eurotech in 1999. It was a project to monitor the oil pipeline across deserts. The purpose was to provide data transmissions on a lightweight and little battery power consumption protocol because the connection between the devices was through an extremely expensive satellite link. In 2013, IBM submitted MQTT version 3.1 [14] to be the OASIS (Organization for the Advancement of Structured Information Standards) specification. Historically, instead of message queuing, the "MQ" in "MQTT" originally is the name of the IBM MQ product line. It applies a publish/subscribe mechanism to minimize the payload and overhead. Now, MQTT is widely used in IT departments and available in many open sources or programming languages. It is used not only to monitor oil pipelines in the energy industry mentioned above but also to monitor or send commands in chemical, medical, autonomous driving, and other industries. Even Facebook Messenger applies MQTT which is a common communication software. Therefore, the security of the MQTT protocol is important.

In the default situation, the transmissions with MQTT on port 1883 are not encrypted. For the sensitive information contained in the message, the MQTT specification recommends using the TLS protocol on port 8883 for protecting the data. Although most brokers and MQTT platforms support the TLS protocol, Mathews *et al.* [13] and Sadio *et al.* [18] mentioned that CPU usage and communication overhead come at the expense of limited devices. Once a message is published, TLS protocol needs to perform a handshake process. Although an IoT payload is small, it has to be transmitted frequently. If TLS protocol is often used, it always needs to reconnect and perform a handshake process due to the unstable signal of the IoT connection. That consumes a lot of power and computation time. Besides, the TLS session keeps connecting until the MQTT client finishes its work. In this case, it is not beneficial for short-lived connection. According to TLS 1.2 [9], a handshake protocol spends approximately 250 microseconds in the six steps (Figure 3). Even if with the improvements, TLS version 1.3 [12] still takes at least 150 microseconds. Therefore, it takes up most of the

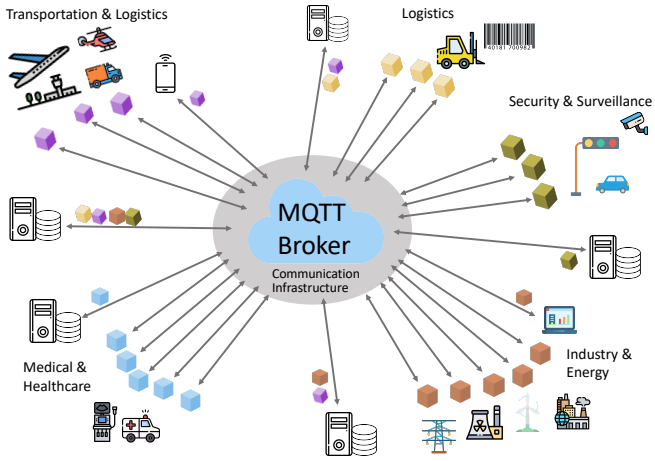

Fig. 2. MQTT used in the IoT M2M industry

computation and time for those devices.

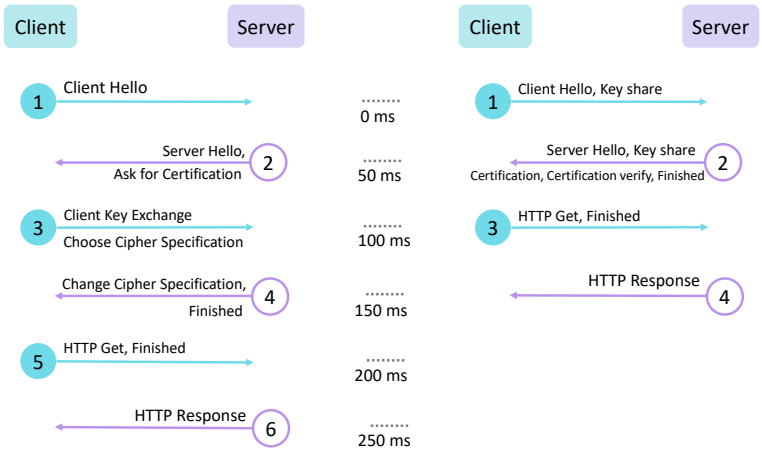

Fig. 3. The time cost of TLS version 1.2 and version 1.3

Concerning the IoT devices that are unsuitable for TLS protocol, payload encryption is a more appropriate method to protect messages. TLS protocol encrypts the payload of the TCP packet which is the entire MQTT packet including the header. In contrast with encrypting the whole MQTT packet, payload encryption only encrypts the content of the MQTT messages, the broker can directly check the MQTT header (Figure 4) without decryption. In 2015, Singh *et al.*

[20] proposed an attribute-based encryption (ABE) scheme to encrypt the messages of MQTT. Except for the original hierarchical topic tree, Singh *et al.* [20] needs to build another access tree for the attributes or identities of Subscriber. The access trees may not be shared, so Publisher or Broker need more space to store the access tree. Some of the IoT devices are resource-constrained, they may not have enough space to store or create the access trees. Singh *et al.*'s scheme needs to create attributes for Subscriber and convert them into an access structure, which requires a lot of time to compute and space to store. Moreover, each access tree may represent only a topic. The more topics exist, the more access structures Broker needs to store.

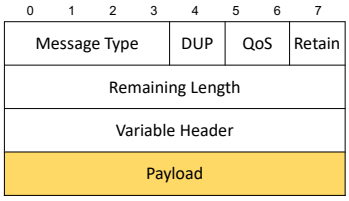

Fig. 4. The packet of MQTT

1.1 Related Work

In 2015, Singh *et al.* [20] propose a payload encryption scheme using key-policy attribute-based encryption (KP-ABE) [5] and ciphertext-policy attribute-based encryption (CP-ABE) [2], called SMQTT. They also demonstrate the feasibility of their protocol for various IoT environments through simulations to evaluating the performance. In their scheme, using CP-ABE scheme has higher complexity (storage and computation) than the KP-ABE one. In their experiment, they compare not only the scheme with the ABE scheme from X. Wang *et al.* [21], but also the performance between CP-ABE and KP-ABE. Message M is encrypted by 128 bit AES key that is encrypted by KP-ABE or CP-ABE. However, Singh *et al.*'s scheme [20] does not present the details about how the parameters set and the security proof work.

1.2 Contributions

To solve the problems mentioned above, we propose payload encryption from hierarchical identity-based encryption (HIBE) for MQTT, called MQHIBE. Differing from Singh *et al.*'s scheme [20], hierarchical topics of MQTT perfectly match the HIBE. Compared with the MQTT messages protected by the TLS protocol and Singh *et al.*'s scheme [20], the proposed MQHIBE scheme is more efficient and achieves the property of hierarchical topics. Furthermore, as we will show in Section 5, the proposed scheme has better performance in time complexity and it can defend replay attacks. If an attacker resends the message, nothing will happen to the system, the subscriber just receives the same message again. Moreover, we have formally proven that the proposed MQHIBE scheme is secure in the standard model. It is worth noting that, MQTT may not be the only application for the proposed scheme. The proposed scheme may be suitable for the environments with a hierarchical data structure inside, such as Named Data Networking (NDN) [1, 17]. NDN is a novel networking architecture, where hierarchical named data are used for communication, instead of using IP. Besides, NDN has been deployed on IoT [6] with MQTT as well. We believe that the proposed scheme would also a solution suitable for protecting the privacy in NDN.

1.3 Organization

In Section 2, we describe the formal definitions of the MQHIBE scheme and the complexity assumptions used in the proofs. In Section 3, we provide a detailed description of the MQHIBE scheme. In Section 4, we provide the security models and proofs of the proposed MQHIBE scheme. The comparisons and the conclusion are presented in Section 5 and Section 6.

2 PRELIMINARIES

This section provides the background knowledge, and the definition of hierarchical ID-based encryption (HIBE) followed by certain mathematical assumptions used in the security proofs.

2.1 MQTT

MQTT is a publish/subscribe protocol that runs on top of TCP [8] network. A message packet in MQTT is presented as Figure 5. In an MQTT protocol, there are three main characters: Publisher, Broker, Subscriber, and the message transports via topics. Any Publisher or Subscriber that connects to the centralized Broker over networks is considered to be a client. In MQTT, messages are organized in a hierarchy of topics as shown in Figure 6. We briefly introduce the terminologies below.

- **Subscriber:** A client that subscribes to a topic or topics from Broker.
- **Publisher:** A client that publishes a message to Broker with the corresponding topic.
- **Broker:** Broker is a server that receives the messages sent from Publisher and forwards them to Subscriber. The clients must actively connect to Broker, then Broker will hold the connection to persistent clients. There are several platforms of MQTT Brokers include HiveMQ, AWS IoT.
- **Topic:** A topic of an MQTT Broker is a connection between Subscriber and Publisher. Each message belongs to a certain topic. A message topic is composed of different topic levels separated by a slash and represented as a string like Home/Yard/Pond/Water Level. Topics are different due to uppercase and lowercase, and the permutation of the topic is also important. If there is a topic Home/Yard/Pond, the message with topic Home/Pond/Yard will not be accepted by Broker because of the exchange between Pond and Yard.

Connecting with Broker, Subscriber sends a Subscribe packet to Broker to create one or more subscriptions. When Publisher sends a message to Broker, Broker will forward the messages to Subscriber that match those subscriptions. Publisher need not to know where Subscriber is, and Subscriber need not to know who sends the message. If Broker receives a message with a topic for which there are no current Subscriber, it will discard the topic unless Publisher indicates that the topic is to be retained.

2.1.1 Wildcard Characters. Subscriber can not only subscribe to an exact topic but also use a wildcard character to subscribe to multiple topics concurrently. A wildcard character can only be used for the topic subscription. There are two kinds of wildcards in MQTT: single-level wildcard and multi-level wildcard, which are denoted by the symbols "+" and "#", respectively.

- **Single-Level Wildcard (+)**: A single-level wildcard can replace a topic level. The symbol "+" represents a single-level wildcard in the MQTT topic, and it can be put at any level of the topic. For example, as shown in Figure 7, a subscription to Home/Yard/+ can produce the following results:

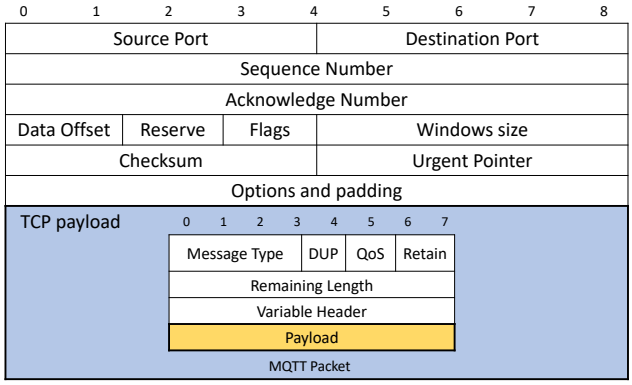

Fig. 5. An MQTT packet on a TCP network

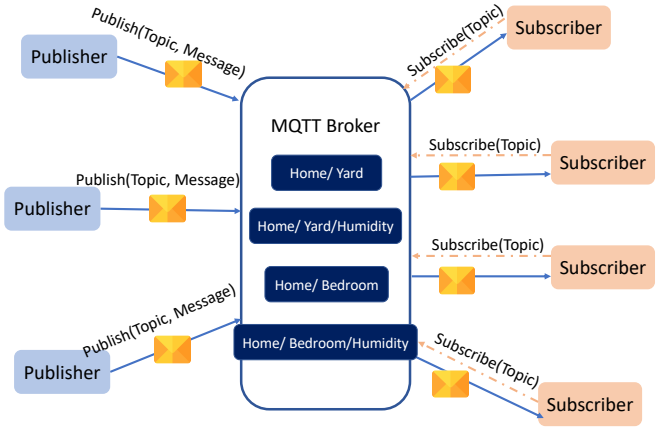

Fig. 6. The message transport in MQTT

- Home/Yard/Pond
- Home/Yard/PIR 1
- Home/Yard/PIR 2
- Home/Yard/Temperature
- Home/ Yard/ Humidity

Note that the symbol is allowed to be placed in the middle of the topic such as Home/+/Humidity, which indicates "Home/Yard/Humidity" and "Home/Bedroom/Humidity" in Figure 7.

- **Multi-Level Wildcard (#)**: The multi-level wildcard can replace many topic levels at a time, and it must be placed as the last character. For a subscription to the topics with a multi-level wildcard, Subscriber will

receive all the messages that own the same prefix to the topic. If a topic contains only a multi-level wildcard, it means a subscription to all the topics. For example, as shown in Figure 7, a topic Home/Bedroom/#, it means subscriptions below:

- Home/Bedroom
- Home/Bedroom/Temperature
- Home/Bedroom/Humidity

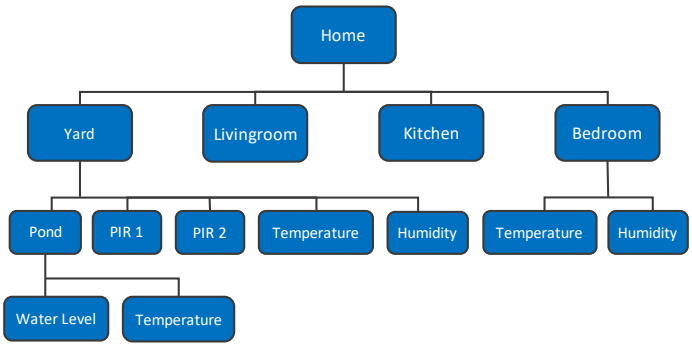

Fig. 7. The levels of hierarchical topics

2.2 Hierarchical ID-Based Encryption (HIBE)

Jeremy Horwitz and Ben Lynn proposed the first HIBE scheme [7] in 2002 which is a two level structure scheme. HIBE is an extension form of IBE [4] which is a public-key cryptography.

Definition 2.1. An HIBE scheme consists of the following probabilistic algorithms:

- **Setup ($SK_0, \mathcal{P}$) :** PKG runs the function and a security parameter to generate a master key MK_0 (which we also call the level-0 key) and a set $\mathcal{P}$ of system parameters.
- **KeyGen** $(SK_{i-1}, ID_i, \mathcal{P}) \rightarrow SK_i$ **:** The algorithm takes system parameters $\mathcal{P}$, master secret SK_{i-1}, and identity ID_i as input. It outputs a private key SK_i corresponding to identity ID_i where i denotes the i^{th} level of the ID.
- **Encrypt** $(\mathcal{P}, ID_i, M) \rightarrow CT$ **:** A data owner runs the algorithm to generate a ciphertext CT. It takes the set of system parameters $\mathcal{P}$, a message M, and an identity ID_i as input. Then, the data owner can generates a ciphertext CT.
- **Decrypt** $(\mathcal{P}, ID_i, CT, SK_i) \rightarrow M$ **:** A receiver performs the algorithm to obtain the message. It takes ciphertext CT, system parameters $\mathcal{P}$, identity ID_i and private key SK_i as input. Eventually, the receiver can get message M.

2.3 Named Data Networking

Named data networking (NDN) is one of the promising candidates for information-centric networking [22]. In NDN, hierarchical data names are emphasized instead of IP addresses. A data name would consist of producer ID, date, unique data identifier, and other necessary information, for instance, "Bob-123456/Sept2022/paper/abc.pdf".

producer ID Date Data ID

2.4 Bilinear Mapping

Let G and G_1 be two cyclic multiplicative groups of prime order p. A bilinear mapping $e : G \times G \rightarrow G_1$ satisfies the following properties [4] in which g is a generator of G.

- **Bilinearity:** $e(g^a, g^b) = e(g, g)^{ab}$, $\forall a, b \in \mathbb{Z}_p$.
- **Non-Degeneracy:** The function does not map all pairs in $G \times G$ to the identity of G_1. Since G and G_1 are groups of the same prime order, it implies that if g is a generator of G, then $e(g, g)$ is a generator of G_1.
- **Computability:** There exists an efficient algorithm to compute $e(g, g)$, $\forall g \in G$.

2.5 ℓ-Weak Bilinear Diffie-Hellman Inversion (ℓ-wBDHI) Assumption

Let G and G_1 be two cyclic groups of prime order p, g be a generator of G, and $e : G \times G \rightarrow G_1$ be a bilinear mapping.

Definition 2.2. Given $< G, G_1, e, g, h, g^{\alpha}, g^{\alpha^2}, \cdots, g^{\alpha^{\ell}}, Z >$ for some random $\alpha \in \mathbb{Z}_p^*$ and $g, h \in G$, decide if Z is equal to $e(g, h)^{\alpha^{\ell+1}}$.

Definition 2.3. An algorithm $\mathcal{A}$ with an output $b' \in \{0, 1\}$ is said to have the advantage ϵ in solving the ℓ-wBDHI problem if

$$|\Pr[\mathcal{A}(g, h, \vec{y}, e(g, h)^{\alpha^{\ell+1}})] = 1 - \Pr[\mathcal{A}(g, h, \vec{y}, Z)] = 1| \geq \epsilon$$

where $\vec{y} = (g^{(\alpha^i)})_{i=1,\ldots,\ell} \in G^{\ell}$, $\alpha \in_R \mathbb{Z}_p$, $g, h \in G$ and $Z \in_R G_1$. We say that the ℓ-wBDHI assumption [3, 19] holds if no polynomial-time algorithm has non-negligible advantage in solving the ℓ-wBDHI problem.

3 THE PROPOSED MQHIBE SCHEME

In this section, we demonstrate a secure scheme based on hierarchical ID-based encryption (HIBE) [3] for the MQTT protocol used in IoT environments, called MQHIBE. Our scheme only encrypts MQTT messages to publish, and thus it will not modify the MQTT structure or cause other problems. Our are four algorithms in our scheme: *Setup, Subscription, Publication, Reception*. The system model of the proposed scheme is illustrated in Figure 8, where Broker is considered honest-but-curious. The notations used in the proposed scheme are shown in TABLE 1.

In the proposed scheme, Publisher and Subscriber are the clients who have been authenticated by Broker. Publisher can be imagined as a sensor, e.g., a thermometer, and it periodically sends out the message about temperatures. Subscriber can be imagined as a smartphone or a device to record temperatures. When Publisher sends a message, and Broker will forward it to Subscriber. In the proposed scheme, the public encryption key for a topic $T_1/T_2/\cdots/T_q$ is viewed as a vector in $(\mathbb{Z}_p^*)^q$. This can be done by regarding T_i as the corresponding integer of its binary representation.

3.1 Setup Algorithm

Broker plays the role of the public key generator (PKG) to generate the public parameters the master secret key as follows. Let ℓ be the maximum depth of HIBE.

(1) Construct the parameters for bilinear map $e : G \times G \rightarrow G_1$, where G is a bilinear group of prime order p.
(2) Choose a generator $g \in G$, a number $\alpha \in \mathbb{Z}_p$ at random and set $g_1 = g^{\alpha}$.
(3) Select a collision resistant hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_p^*$.
(4) Choose random elements $\{c_1, c_2, h_1, ..., h_{\ell}\} \in G$.
(5) Set public parameters $params = (g, g_1, c_1, c_2, h_1, ..., h_{\ell})$ and a master secret key c_1^{α}.

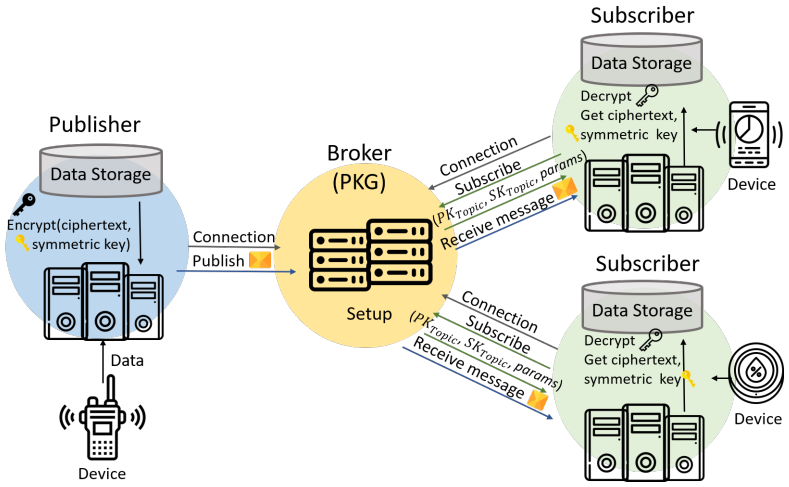

Fig. 8. The sysyem model of the proposed MQHIBE scheme

Table 1. The Notations

Notation	Meaning
G	a cyclic multiplicative group of prime order p
G_1	a cyclic multiplicative group of prime order p
e	a bilinear mapping; $e : G \times G \rightarrow G_1$
PK_{Topic}	a public key, $PK_{Topic} = (T_1/T_2/\cdots/T_q) \in (\mathbb{Z}_p^*)^q$
SK_{Topic}	a secret key to the public key PK_{Topic}.
$PK_{Topic\|q-1}$	a public key at the $(q-1)$-th level, $PK_{Topic\|q-1} = (T_1/T_2/\cdots/T_{q-1}) \in (\mathbb{Z}_p^*)^{q-1}$
$SK_{Topic\|q-1}$	a secret key to the public key $PK_{Topic\|q-1}$.
SE	a symmetric key encryption algorithm
SD	a symmetric key decryption algorithm
$\mathcal{K}$	the symmetric key space
H	a collision resistant hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p^*$.
M	a message
CT	a ciphertext
ℓ	the maximum depth of the HIBE
q	the q-th level of the HIBE

(6) Choose and publish a secure symmetric encryption/decryption algorithms $(SE, SD, \mathcal{K})$ where the key space $\mathcal{K} = G_1$.

3.2 Publication Algorithm

Publisher encrypts message M using symmetric encryption k. Then, Publisher encrypts symmetric key k with the corresponding PK_{Topic} and a random number s as follows. Finishing the encryption, Publisher sends ciphertext CT to Broker.

(1) Generate a symmetric key $k \in \mathcal{K}$.

(2) Let the public key $PK_{Topic} = (T_1/T_2/\cdots/T_q) \in (\mathbb{Z}_p^*)^q$.
(3) Choose random $s \in \mathbb{Z}_p$.
(4) Compute $CT = (e(g_1, c_1)^s \cdot k, g^s, (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^s, SE_k(M))$.
(5) Send CT to Broker.

3.3 Subscription Algorithm

When Subscriber sends a Subscribe packet to Broker, Broker generates the corresponding secret key to Subscriber. The algorithm takes public key PK_{Topic}, master secret key c_1^α, and public parameters $params$ as input. The details are shown as follows.

(1) Choose a random $r \in \mathbb{Z}_p$.
(2) Compute secret key SK_{Topic} under PK_{Topic}, where $PK_{Topic} = (T_1/T_2/\cdots/T_q) \in (\mathbb{Z}_p^*)^q$,
$SK_{Topic} = (c_1^\alpha \cdot (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^r, g^r, h_{q+1}^r, \cdots, h_\ell^r)$.
(3) Send (PK_{Topic}, SK_{Topic}) to Subscriber.

Subscription Algorithm with Multi-Level Wildcard Character #: We next discuss the case when Subscriber submits a topic with multi-level wildcard character. The most significant feature of HIBE is that the secret key of the children can be generated from the parent node's secret key. When Subscriber sends a Subscribe packet with # to Broker, Broker generates the corresponding secret key and the parameters, and then send the public keys, the secret key, and the parameters back to Subscriber.

For example, assume that there are the subscription of the two topics are at the $(q-1)$-th and q-th levels separately, and the two topics are parent-child relationships. The secret key at the q-th level can be generated from the parent topic at the $(q-1)$-th level. The public key and secret key of the parent topic at $(q-1)$-th level are represented as $PK_{Topic|q-1}, SK_{Topic|q-1}$ below. Let $PK_{Topic|q-1} = (T_1/T_2/\cdots/T_{q-1})$. Broker takes a random r', public key $PK_{Topic|q-1}$, master secret key c_1^α, and public parameters $params$ as input to generate secret key $SK_{Topic|q-1}$. Then, Broker sends t, public key $PK_{Topic|q}$, parent secret key $SK_{Topic|q-1}$, and public parameters $params$ to Subscriber. The details are shown as follows.

(1) Choose a random number $r \in \mathbb{Z}_p$ for SK_{Topic}.
(2) Compute the secret key of the parent node at the $(q-1)$-th level,
$SK_{Topic|q-1} = (c_1^\alpha \cdot (h_1^{T_1} \cdots h_{q-1}^{T_{q-1}} \cdot c_2)^{r'}, g^{r\prime}, h_q^{r\prime}, \cdots, h_\ell^{r\prime}) = (a_0, a_1, b_q, \cdots, b_\ell)$.
(3) Choose a random number $t \in Z_p$, and set $r = r' + t$.
(4) Send $t, SK_{Topic|q-1}$ and PK_{Topic} to Subscriber.

Receiving the message from Broker, Subscriber gets t, $params$, and the key pairs $(PK_{Topic|q-1}, SK_{Topic|q-1})$ of the parent topic at level $(q-1)$-th. and it compute the secret key as
$SK_{Topic} = (a_0 \cdot b_q^{T_q} \cdot (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^t, a_1 \cdot g^t, b_{q+1} \cdot h_{q+1}^t, ..., b_\ell \cdot h_\ell^t)$.

3.4 Reception Algorithm

Upon receiving ciphertext CT from Publisher, Broker forwards it to whom subscribes to the same topic. Subscriber uses secret key SK_{Topic} to decrypt ciphertext CT and gets symmetric key k and encrypted message $SE_k(M)$. Utilizing symmetric key k, Subscriber can decrypt $SE_k(M)$ and get message M. The details are shown as follows.

(1) Let $CT = (e(g_1, c_1)^s \cdot k, g^s, (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^s, SE_k(M)) = (A, B, C, D)$.

(2) Let $SK_{Topic} = (c_1^{\alpha} \cdot (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^r, g^r, h_{q+1}^r, \cdots, h_\ell^r) = (a_0, a_1, b_{q+1}, \cdots, b_\ell)$.

(3) Compute

$$\frac{e(a_1, C)}{e(B, a_0)} = \frac{1}{e(g_1, c_1)^s}$$

and retrieve the symmetric key

$$k = A \cdot \frac{e(a_1, C)}{e(B, a_0)}.$$

(4) To retrieve the message, compute

$$M = SD_k(D).$$

Correctness of decryption of cyphertext CT is demonstrated as follows.

$$\begin{aligned}
&\frac{e(a_1, C)}{e(B, a_0)} \\
&= \frac{e(g^r, (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^s)}{e(g^s, c_1^{\alpha}(h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^r)} \\
&= \frac{e(g^r, (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^s)}{e(g^s, c_1^{\alpha}) \cdot e(g^s, (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^r)} \\
&= \frac{e(g^r, (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^s)}{e(g^s, c_1^{\alpha}) \cdot e(g^r, (h_1^{T_1} \cdots h_q^{T_q} \cdot c_2)^s)} \\
&= \frac{1}{e(g, c_1)^{s\alpha}} \\
&= \frac{1}{e(g^{\alpha}, c_1)^s} \\
&= \frac{1}{e(g_1, c_1)^s}.
\end{aligned}$$

Compute symmetric key k

$$k = A \cdot \frac{e(a_1, C)}{e(B, a_0)} = e(g_1, c_1)^s \cdot k \cdot \frac{1}{e(g_1, c_1)^s}$$

and get message M

$$M = SD_k(D).$$

4 SECURITY PROOF

In this section, the security model and security proof are given for the proposed MQHIBE scheme.

4.1 Security Model

Definition 4.1. **The IND-sID-CPA Game**. Let $\mathcal{A}$ be a probabilistic polynomial-time (PPT) attacker. $\mathcal{A}$ interacts with a challenger C in the following game.

Initialization. $\mathcal{A}$ first outputs a topic $PK^*_{Topic} = (T^*_1/T^*_2/\cdots/T^*_m) \in (\mathbb{Z}^*_p)^m$ of depth $m \leq \ell$ that it intends to attack. One may note that l is the maximum depth of the proposed HIBE as TABLE 1 mentioned. Assuming that PK^*_{Topic} is a vector of length ℓ. If $m \leq \ell$, C pads PK^*_{Topic} with $(\ell - m)$ zeroes on the right to make it a constant vector of length ℓ.

Setup. C runs the *Setup* algorithm to generate $params$ and msk. C sends system $params$ to $\mathcal{A}$, and keep msk secret.

Phase 1. $\mathcal{A}$ adaptively issues the following queries.

- Subscription(PK_{Topic}): $\mathcal{A}$ sends a topic PK_{Topic} to C, C generates the private key SK_{Topic} with the corresponding PK_{Topic} by running *Subscription* algorithm. Then, C returns the SK_{Topic} to $\mathcal{A}$. Note that $\mathcal{A}$ is not allowed to sends a topic such that $PK_{Topic} = PK^*_{Topic}$, or PK_{Topic} is a prefix of PK^*_{Topic}.
- Publication(PK_{Topic}, M): $\mathcal{A}$ sends a topic PK_{Topic} and a message M to C. Then, C returns a ciphertext CT to $\mathcal{A}$.

Challenge. $\mathcal{A}$ outputs two equal length messages (M_0, M_1) to C where M_0, M_1 are different messages. C randomly picks $\beta \in \{0, 1\}$ and computes CT^* = with the *Publication* algorithm with $params, PK^*_{Topic}, M_b$. Finally, C sends CT^* to $\mathcal{A}$.

Phase 2. $\mathcal{A}$ issues the queries the same as defined above in *Phase 1.*

Guess. Finally, $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$ and wins the game if $\beta' = \beta$.

The advantage of $\mathcal{A}$ winning the game is defined as

$$\mathbf{Adv}^{\text{IND-sID-CPA}}(\mathcal{A}) = \left| Pr[\beta = \beta'] - \frac{1}{2} \right|.$$

A scheme is said to be IND-sID-CPA secure if there exists no polynomial-time attacker that can win the IND-sID-CPA game with non-negligible advantage.

4.2 IND-sID-CPA Security

In this section, we prove that the proposed MQHIBE scheme is IND-sID-CPA secure under the ℓ-wBDHI assumption.

Theorem 4.2. *The proposed MQHIBE scheme is IND-sID-CPA secure if the ℓ-wBDHI assumption holds.*

Proof. The proof below is based on proof by contradiction. Assuming that the proposed scheme is not IND-sID-CPA secure, that is, there exists a PPT adversary $\mathcal{A}$ that wins the IND-sID-CPA game with a non-negligible advantage. Then, we can construct a polynomial-time algorithm C that owns non-negligible advantage in solving the ℓ-wBDHI problem.

First, C is given an instance of the ℓ-wBDHI problem $(g, h, \vec{y}, Z)$, where $\vec{y} = (y_i)_{i=1,\ldots,\ell} = (g^{(\alpha^i)})_{i=1,\ldots,\ell}$. C simulates the game for $\mathcal{A}$ as follow.

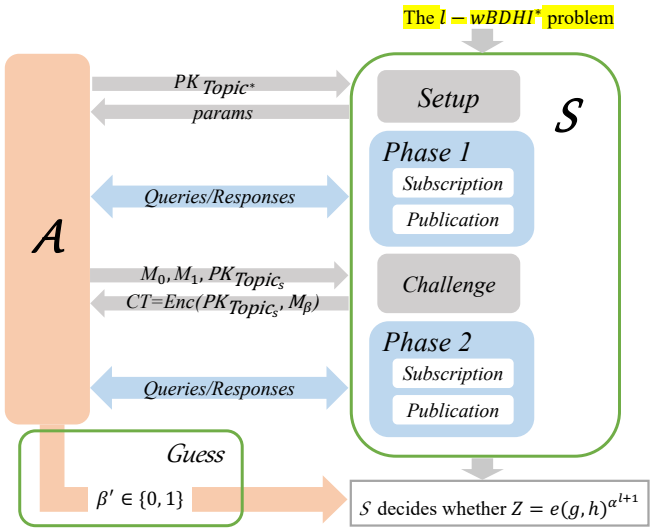

Fig. 9. The IND-sID-CPA game

Initialization. $\mathcal{A}$ outputs a target topic $PK^*_{Topic} = (T_1^*/T_2^*/\cdots/T_m^*) \in (\mathbb{Z}_p^*)^m$ for depth $m \leq \ell$.

Setup. C performs as follows.

(1) Choose random γ in $\mathbb{Z}_p$, set $g_1 = y_1 = g^\alpha$, $c_1 = y_\ell \cdot g^\gamma = g^{\gamma+(\alpha^\ell)}$.
(2) Choose $\gamma_1, \cdots, \gamma_\ell$ in $\mathbb{Z}_p$ at random.
(3) For $i = 1, \cdots, \ell$, compute $h_i = g^{\gamma_i}/y_{\ell-i+1}$.
(4) Choose random δ in $\mathbb{Z}_p$, $c_2 = g^\delta \cdot \prod_{i=1}^{\ell} y_{\ell-i+1}^{T_i^*}$.
(5) Implicitly set the master key $c_1^\alpha = g^{\alpha(\alpha^\ell+\gamma)} = y_{\ell+1}y_1^\gamma$.

C chooses a secure symmetric encryption scheme (SE, SD) with key space $\mathcal{K} = G_1$, and outputs $\{g, g_1, c_1, c_2, h_1, \cdots, h_\ell\}$ along with $(SE, SD, \mathcal{K})$.

Phase 1. In this phase, $\mathcal{A}$ issues the queries below:

- Subscription:
  C takes a topic $PK_{Topic|u} = (T_1/T_2/\cdots/T_u) \in (\mathbb{Z}_p^*)^u$ as input, with $u \leq \ell$. Since $PK_{Topic|u}$ is not a prefix of PK^*_{Topic}, there must be a minimal index $k \in \{1, 2, \ldots, u\}$ such that $T_k \neq T_k^*$; otherwise $PK_{Topic|u}$ would be a prefix of PK^*_{Topic}. In other word, we have $T_i = T_i^*$ for $i < k$. C then derives the secret key $PK_{Topic|k}$, where $PK_{Topic|k}$ is a prefix of $PK_{Topic|u}$, and C can construct the private key for the requested $PK_{Topic|u} = (T_1/T_2/\cdots/T_k/\cdots/T_u)$ as the shown in the proposed scheme. More precisely, C randomly chooses $\tilde{r}$ from $\mathbb{Z}_p$

and compute the secret secret key $(a_0, a_1, b_{k+1}, \ldots, b_\ell)$ for $PK_{Topic|k}$ with

$$\begin{aligned} a_0 &= y_1^{\gamma} \cdot \left(y_k^{\frac{\delta+\sum_{i=1}^{k} T_i\gamma_i}{T_k - T_k^*}} \prod_{i=k+1}^{\ell} y_{\ell-i+k+1}^{T_i^*} \right) \\ &\quad \cdot \left(g^{\delta+\sum_{i=1}^{k} T_i\gamma_i} \prod_{i=k+1}^{\ell} y_{\ell-i+1}^{T_i^*} \right) \cdot y_{\ell-k+1}^{\tilde{r}(T_k^* - T_k)}, \\ a_1 &= y_k^{\frac{1}{T_k - T_k^*}} \\ b_j &= \left(y_k^{\gamma_j} / y_{\ell-j+k+1} \right)^{\frac{1}{T_k - T_k^*}} \cdot \left(g^{\gamma_j} / y_{\ell-j+1} \right)^{\tilde{r}}, \end{aligned}$$

for $j = k+1, \ldots, \ell$. By implicitly setting $r = \frac{\alpha^k}{(T_k - T_k^*)} + \tilde{r}$, $(a_0, a_1, b_{k+1}, \ldots, b_\ell)$ is a valid secret key for $PK_{Topic|k}$. The details of the correctness analysis are shown in Appendix A.

- Publication:

  C takes the topic $PK_{Topic|u}$ and a message M as input, and follows the *Encryption* algorithm in Section 3.2 to encypt the message.

  (1) Choose a symmetric key k.
  (2) Generate the ciphertext $CT = (e(g_1, c_1)^r \cdot k, g^r, (h_1^{T_1} \cdots h_u^{T_u} \cdot c_2)^r, SE_k(M))$ for a randomly chosen r.

Challenge.

$\mathcal{A}$ sends (M_0, M_1) and PK^*_{Topic} to C where M_0, M_1 are two different messages with the same length. Then, C randomly chooses $\beta \in \{0, 1\}$ at random and a symmetric key $k \in G_1$, and computes

$$CT^* = (k \cdot Z \cdot e(y_1, h^{\gamma}), h, h^{\delta+\sum_{i=1}^{l} T_i^*\gamma_i}, SE_k(M_\beta)).$$

Finally, CT^* is transmitted to $\mathcal{A}$.

Phase 2.

$\mathcal{A}$ and C interacts to each other the same as *Phase 1.*

Guess.

Finally, $\mathcal{A}$ outputs $\beta' \in \{0, 1\}$. If $\beta' = \beta$, then C outputs 1. Otherwise, C outputs a uniformly random bit. If $Z = e(g, h)^{\alpha^{l+1}}$, by implicitly setting the randomness s used in encryption as $\log_g h$, i.e. $s = \log_g h$, we have that CT^* is a valid ciphertext. More precisely,

$$\begin{aligned} k \cdot Z \cdot e(y_1, h^{\gamma}) &= k \cdot e(g, h)^{(\alpha^{l+1})} \cdot e(y_1, h^{\gamma}) \\ &= k \cdot e(g^{\alpha}, h^{\alpha^{\ell}} \cdot h^{\gamma}) \\ &= k \cdot e(g_1, c_1)^s, \end{aligned}$$

and

$$\begin{aligned} h^{\delta+\sum_{i=1}^{l} T_i^*\gamma_i} &= (g^{\delta+\sum_{i=1}^{l} T_i^*\gamma_i})^s \\ &= [(g^{\delta} \cdot \textstyle\prod_{i=1}^{\ell} y_{\ell-i+1}^{T_i^*}) \cdot \prod_{i=1}^{\ell} (g^{T_i^*\gamma_i} / y_{\ell-i+1}^{T_i^*})]^s \\ &= (c_2 \cdot \textstyle\prod_{i=1}^{\ell} h_i^{T_i^*})^s. \end{aligned}$$

In this case, we have that

$$\Pr[C(g, h, \vec{y}, Z = e(g, h)^{\alpha^{\ell+1}}) = 1] = \mathbf{Adv}^{\text{IND-sID-CPA}}(\mathcal{A}) + \frac{1}{2}.$$

Otherwise, if Z is a random element in G_1, then CT^* is composed of random elements, since SE is a secure symmetric encryption algorithm. As a result, CT^* reveals no information about M_β, and thus $\mathcal{A}$ has no advantage in winning the game. Therefore, we have that, in this case, $\Pr[C(g, h, \vec{y}, Z \in_R G_1) = 1] = \frac{1}{2}$.

Finally, we have that, the advantage of C in solving ℓ-wDBHI problem is

$$\begin{aligned} & \Big|\Pr[C(g, h, \vec{y}, Z = e(g,h)^{\alpha^{\ell+1}}) = 1] \\ - \quad & \Pr[C(g, h, \vec{y}, Z \in_R G_1) = 1]\Big| \\ = \quad & \Big|(\mathbf{Adv}^{\text{IND-sID-CPA}}(\mathcal{A}) + \tfrac{1}{2}) - \tfrac{1}{2}\Big| \\ = \quad & \mathbf{Adv}^{\text{IND-sID-CPA}}(\mathcal{A}). \end{aligned}$$

As a result, C solves the ℓ-wBDHI problem with non-negligible advantage within polynomial time, if $\mathcal{A}$ win the game with non-negligible advantage. □

5 COMPARISON

In this section, we compare the proposed scheme with [20] and [15] in terms of properties and performances. We summarize the functionality comparison between [20] in TABLE 2. The comparison with [20] and MQTT standard using TLS protocol are presented in TABLE 5 and TABLE 6. Some computation costs for cryptographic primitives are shown in TABLE 4.

5.1 Properties Comparison

Our MQHIBE scheme adopts the properties of hierarchical encryption, and its security is also guaranteed in Section 4.2. In the following, we present differences from scheme of [20], shown in TABLE 2.

- **Encryption for Hierarchical Structure**: As an IoT data protocol, MQTT publishes/subscribes the messages that rely on hierarchical topics. Once a client publishes a message on a specific topic, Broker will forward the message that matches the topic subscription. An MQTT topic is a UTF-8 string that consists of one or more topic levels. Every topic level is separated by a slash character that makes the topic presence hierarchically in the string. Compared with Singh *et al.*'s scheme [20], ours is more tailored for MQTT.
- **Security**: In chosen-plaintext attacks (CPA), the adversary can choose several plaintexts to be encrypted and have access to the generated ciphertexts. In chosen-ciphertext attacks (CCA), the adversary can additionally gather information by a decryption oracle with chosen ciphertexts. The CCA security is more strong than the CPA security since an CCA adversary is allowed to access more resources. Besides, STD and ROM denote *the standard model* and *the random oracle model* respectively. In the standard model, the adversary is only restricted to reasonable runtime and computation ability. In the random oracle model, there is an additional restriction that the adversary is asked to access hash oracles to obtain hash values, rather than compute the values by itself. Due to the additional restriction, the standard model is more preferable for a security proof.

5.2 Performance Evaluation and Discussion

We analyze the performance of the encryption and decryption algorithms via python libraries on a Ubuntu 18.04.4 LTS Linux system with Intel Core i9-9940X 3.30GHz. Standard MQTT with TLS protocol encrypts the payload of TCP packets, which is an entire MQTT packet. The cryptographic primitives of TLS protocol apply to version 1.2 and the

Table 2. Properties Comparison

Scheme	Hierarchical	Encryption	Assumption	Security proof
Singh *et al.* [20]	No	CP-ABE [2]	None	ROM/CPA
		KP-ABE [5]	DBDH	STD/CPA
The MQHIBE scheme	Yes	HIBE	ℓ-wBDHI	STD/CPA

latest version 1.3. To compare with the protocols of [9, 20] and our MQHIBE, we implement RSA algorithm, SHA-384, AES algorithm, and other primitives via python libraries. The information for the environment is shown in TABLE 3, and the time consumption for each primitive is shown in TABLE 4. We note that AES-GCM is a kind of symmetric cryptosystem extended from AES. We use AES-GCM as the symmetric encryption/decryption algorithms used in each protocols. In the following, we analyze the performance under the scenario that the message is encrypted under the topic Home/Bedroom/Temperature, and a maximum of 3 levels in MQHIBE. The structure for the topics is shown in Fig. 10.

Table 3. Simulation Environment

Operating System	Linux Ubuntu 16.04 LTS 32bit
CPU	Intel(R)Core(TM) i7-4650U CPU @ 1.70GHz
Memory	7.8 GB
Motherboard	Apple Inc. 121.0.0.0.0

Table 4. Computation Costs of Cryptographic Primitives in millisecond (ms)

Notation	Meaning	Key size	Cost
$T_{AES-GCM_{Enc}}$	the cost of an AES-GCM encryption	256 bits	0.003 ms
$T_{AES-GCM_{Dec}}$	the cost of an AES-GCM decryption	256 bits	0.231 ms
T_{ECDHE}	the cost of an ECDHE operation	-	62.972 ms
$T_{RSA_{Enc}}$	the cost of an RSA encryption	2048 bits	2.903 ms
$T_{RSA_{Dec}}$	the cost of an RSA decryption	2048 bits	109.462 ms
$T_{h_{384}}$	the cost of a 384 bits hash operation	-	0.001 ms
T_p	the cost of a pairing operation	-	33.524 ms
T_m	the cost of a modular multiplication in $\mathbb{Z}_q$	-	0.001 ms
T_s	the cost of a scalar multiplication in an additive group or an exponentiation in a multiplicative group	-	0.019 ms
T_a	the cost of an addition in an additive group or a multiplication in a multiplicative group	-	0.025 ms

5.3 Comparison with Singh *et al.*'s ABE-Based Methods

- Singh *et al.* [20] based on CP-ABE [2]:
  According to Figure 10, we construct an access tree of Subscriber's identities for CP-ABE illustrated as Figure 11. There are four attributes only for topic Home/Bedroom/Temperature. If Publisher needs to send another message that is no relation to "temperature" like Home/Bedroom/Humidity, the message cannot use the same access structure shown in Figure 11. Therefore, Broker has to store additional attributes for Subscriber's identities and provides Publisher to generate the access tree.

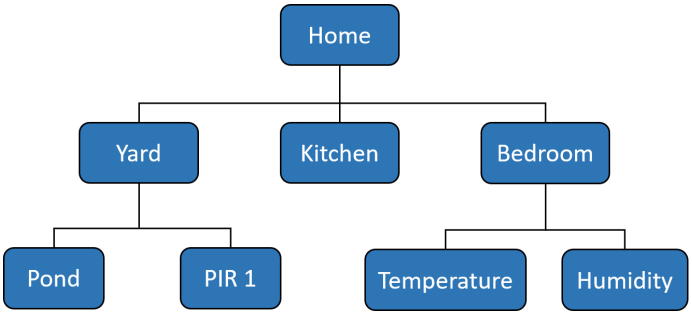

Fig. 10. The Structure of Hierarchical Topics

- **Key Generation**: The cost of key generation for topic Home/Bedroom/Temperature is $T_s + T_m + 4 \cdot (T_s + T_{h_{384}} + T_s + T_s) \approx 13T_s + 4T_{h_{384}} + T_m \approx 0.247 + 0.004 + 0.001 \approx 0.252$ ms.
- **Encryption**: Publisher first generates a symmetric key to encrypt the plaintext, that is, an AES-GCM key. Then, the ABE scheme is used to protect the symmetric key. The cost of generating ciphertext is $T_p + T_a + T_m + T_s + 4 \cdot (T_s + T_{h_{384}} + T_s) + T_{AES-GCM_{Enc}} \approx 9T_s + 4T_{h_{384}} + T_p + T_a + T_m + T_{AES-GCM_{Enc}} \approx 0.171 + 0.004 + 33.524 + 0.025 + 0.001 + 0.003 \approx 33.728$ ms.
- **Decryption**: Using the decryption algorithm of the ABE scheme, we can get the symmetric key, and then recover the palintext. The cost of decrypting the ciphertext is $2 \cdot T_p + T_a + T_m + 7T_a + T_p + 2T_a + T_{AES-GCM_{Dec}} \approx 10T_a + 3T_p + T_m + T_{AES-GCM_{Dec}} \approx 0.25 + 100.572 + 0.001 + 0.231 \approx 101.054$ ms.

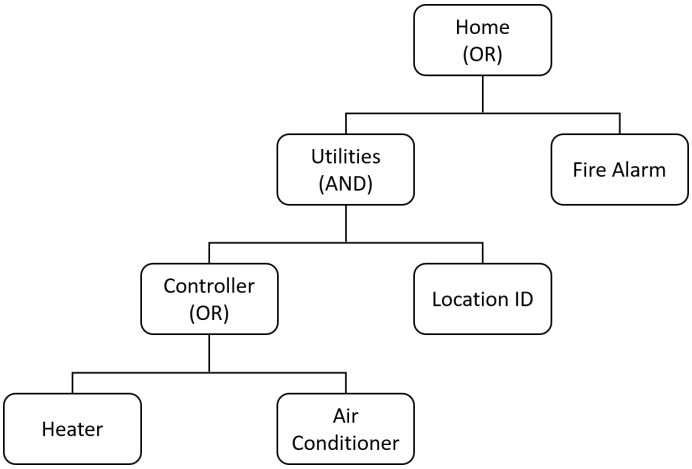

Fig. 11. The access structure of Subscriber's identities in CP-ABE and KP-ABE

- Singh *et al.* [20] based on KP-ABE [5]:
  According to Figure 10, we construct an access tree of Subscriber's identities for KP-ABE illustrated as Figure 11. There are four attributes only for topic Home/Bedroom/Temperature. If Publisher needs to send another message

that is no relation to "temperature" like Home/Bedroom/Humidity, the message cannot use the same access structure shown in Figure 11. Therefore, Broker has to store additional attributes for Subscriber's identities and generates the access tree for Publisher in advance.

- **Key Generation**: The cost of key generation for topic Home/Yard/Pond is $4 \times (T_m + T_s) \approx 4 \times 0.02 \approx 0.08$ ms.
- **Encryption**: The analysis is similar to the CP-ABE case. The cost of generating ciphertext is $T_a + T_s + 4 \cdot T_s + T_{AES-GCM_{Enc}} \approx T_a + 5T_s + T_{AES-GCM_{Enc}} \approx 0.025 + 0.095 + 0.003 \approx 0.123$ ms.
- **Decryption**: The analysis is similar to the CP-ABE case. The cost of decrypting ciphertext is $2 \cdot T_p + T_a + T_m + 4T_a + T_a + T_{AES-GCM_{Dec}} \approx 2T_p + 6T_a + T_m + T_{AES-GCM_{Dec}} \approx 67.048 + 0.15 + 0.001 + 0.231 \approx 67.43$ ms.

- The MQHIBE scheme:
  - **Key Generation**: According to the assumptions, the cost of key generation for three-level topic Home/Yard/Pond is $T_s + T_a + 3 \cdot T_s + 3 \cdot T_a + T_s + T_s \approx 6T_s + 4T_a \approx 0.114 + 0.1 \approx 0.214$ ms.
  - **Encryption**: Publisher first generates an AES-GCM key to encrypt the plaintext, then, uses the MQHIBE encryption algorithm to protect the AES-GCM key. The cost of generating ciphertext is $T_a + 3T_s + T_{AES-GCM_{Enc}} \approx 0.025 + 0.057 + 0.003$ ms ≈ 0.085 ms.
  - **Decryption**: By using the decryption algorithm of the MQHIBE scheme, we can get the symmetric key and recover the plaintext. The cost is $2T_p + 2T_a + T_{AES-GCM_{Dec}} \approx 67.048 + 0.05 + 0.231$ms ≈ 67.329 ms.

Table 5. Performance Comparison with Singh *et al.*'s Scheme

Scheme		Key generation	Encryption cost	Decryption cost
Singh *et al.* [20]	CP-ABE	0.252 ms	33.728 ms	101.054 ms
	KP-ABE	0.08 ms	0.123 ms	67.43 ms
The MQHIBE scheme		0.214 ms	0.085 ms	67.329 ms

5.4 Comparison with TLS

The following comparison is between the standard MQTT with TLS and the proposed MQHIBE scheme via three aspects: Preparation, Encryption cost, Decryption cost. The results are shown in TABLE 6. We assume that the published message of topic is Home/Yard/Pond for the convenience in comparison.

- Standard MQTT with TLS protocol:
  - **Preparation**: In preparation, TLS protocol needs to do handshake protocol and key exchange. The cost of the preparation is $T_{ECDHE} + T_{RSA_{Enc}} + T_{RSA_{Dec}} + 17T_{h_{384}} \approx 62.972 + 2.903 + 109.462 + 0.017 \approx 175.354$ ms
  - **Encryption**: After preparation, Publisher sends the plaintext to Broker. TLS protocol previously encrypts the plaintext before transmission by using symmetric cryptosystem such as AES-GCM. The cost of generating a ciphertext is $T_{AES-GCM_{Enc}} + T_{h_{384}} \approx 0.003 + 0.001 \approx 0.004$ ms.
  - **Decryption**: After receiving the message, Broker decrypts the ciphertext with the symmetric key. If there is a subscription related to the message, Broker needs to create another TLS secure channel to encrypt the plaintext again. The more subscriptions to the topic of the message the more TLS secure channels need to be created. The cost of decrypting ciphertext is $T_{AES-GCM_{Dec}} + T_{h_{384}} \approx 0.231 + 0.001 \approx 0.232$ ms.
- The MQHIBE scheme:

- **Preparation**: In preparation, the MQHIBE scheme needs to perform key generation after *setup*. The cost of key generation for three-level topic Home/Yard/Pond is $T_s + T_a + 3 \cdot T_s + 3 \cdot T_a + T_s + T_s \approx 0.114 + 0.1 \approx 0.214$ ms.
- **Encryption**: The cost of generating ciphertext is $T_a + 3T_s + T_{AES-GCM_{Enc}} \approx 0.025 + 0.057 + 0.003$ ms ≈ 0.085 ms.
- **Decryption**: The cost of decrypting ciphertext is $2T_p + 2T_a + T_{AES-GCM_{Dec}} \approx 67.048 + 0.05 + 0.231$ms ≈ 67.329 ms.

Table 6. Performance Comparison with MQTT using TLS

	Standard MQTT with TLS protocol	The proposed MQHIBE scheme
Preparation	$T_{ECDHE} + T_{RSA_{Enc}} + T_{RSA_{Dec}} + 17T_{h_{384}}$ $\approx 62.972 + 2.903 + 109.462 + 0.017$ ms ≈ 175.354 ms	$T_s + T_a + 3 \cdot T_s + 3 \cdot T_a + T_s + T_s$ $\approx 0.114 + 0.1$ ≈ 0.214 ms
Encryption cost	$T_{AES-GCM_{Enc}} + T_{h_{384}}$ $\approx 0.003 + 0.001$ ms ≈ 0.004 ms	$T_a + 3T_s + T_{AES-GCM_{Enc}}$ $\approx 0.025 + 0.057 + 0.003$ ms ≈ 0.085 ms
Decryption cost	$T_{AES-GCM_{Dec}} + T_{h_{384}}$ $\approx 0.231 + 0.001$ ms ≈ 0.232 ms	$2T_p + 2T_a + T_{AES-GCM_{Dec}}$ $\approx 67.048 + 0.05 + 0.231$ ms ≈ 67.329 ms
Total cost	≈ 175.59 ms	≈ 67.628 ms

All the clients in MQTT are IoT sensors or devices for specific jobs, hence the subscription will not often be canceled or changed. Only when a subscription to new topics occurs, or Broker updates all the keys, Subscriber needs to get a new HIBE or ABE keys from Broker. Unlike the public-key cryptography, MQTT using TLS protocol always needs to perform key exchange before sending the message.

6 CONCLUSION

In consideration of message confidentiality in MQTT, researches presented different encryption mechanisms in the literature. It is a worth-focusing issue because of the rising number of connected IoT devices, and the MQTT protocol has been widely used in recent years. The MQTT specification suggests that either the TLS protocol or other cryptographic schemes is a good option for protecting sensitive messages. Many companies and MQTT platforms choose the TLS protocol to encrypt messages due to the generality and convenience. Yet, the TLS protocol has high computation cost and time consumption. Some researches turned to study other encryption methods, e.g. ABE, and implement them in the MQTT environment, but without detailed and complete security proofs for the schemes.

To cope with the problem, a novel MQTT encryption scheme, i.e. MQHIBE, is designed using hierarchical ID-based encryption during the communications. In an MQTT protocol, every message belongs to a topic which is a hierarchical namespace stored in the broker. This is the reason why the proposed scheme utilized hierarchical ID-based encryption to protect the messages. Different from the scheme with the ABE, it needs to give values to attributes that represent Subscriber. Moreover, every attribute requires a specific value, but the proposed scheme does not need to do so. Furthermore, the proposed scheme meets the need of the subscription by a multi-level wildcard character. The most significant feature of MQHIBE is that the root node can hierarchically generate the private keys of the descendants, and the private key of a node can be generated from the private key of its parent node. As a result, we take the advantage and use it in

a multi-level wildcard character when subscription.

With the advantages mentioned before, the proposed MQHIBE scheme is suitable for MQTT environment and guarantees secure message transmission. We note that, as an independent interest, the proposed scheme would be suitable for privacy preserving in NDN due to the similar hierarchical data structures. In the future, how to achieve the CCA security will be a further study. In addition, the quality of service and quality of message transmission (such as data recovery) in MQTT are an open challenges to be investigated in the near future.

ACKNOWLEDGMENTS

This work was partially supported by the National Science and Technology Council (NSTC) of Taiwan under grants 111-2218-E-110-001-MBK, 110-2923-E-110-001-MY3, and 110-2221-E-004-003, 111-2221-E-004-005. It also was financially supported by the Information Security Research Center at National Sun Yat-sen University in Taiwan and the Intelligent Electronic Commerce Research Center from The Featured Areas Research Center Program within the framework of the Higher Education Sprout Project by the Ministry of Education (MOE) in Taiwan.

REFERENCES

[1] Alexander Afanasyev, Zhenkai Zhu, Yingdi Yu, Lijing Wang, and Lixia Zhang. 2015. The Story of ChronoShare, or How NDN Brought Distributed Secure File Sharing Back. In *2015 IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*. 525–530. https://doi.org/10.1109/MASS.2015.59

[2] J. Bethencourt, A. Sahai, and B. Waters. 2007. Ciphertext-Policy Attribute-Based Encryption. In *2007 IEEE Symposium on Security and Privacy (SP '07)*. 321–334.

[3] Dan Boneh, Xavier Boyen, and Eu-Jin Goh. 2005. Hierarchical Identity Based Encryption with Constant Size Ciphertext. In *Advances in Cryptology – EUROCRYPT 2005*. Springer Berlin Heidelberg, Berlin, Heidelberg, 440–456.

[4] Dan Boneh and Matt Franklin. 2001. Identity-Based Encryption from the Weil Pairing. In *Advances in Cryptology — CRYPTO 2001*, Joe Kilian (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 213–229.

[5] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. 2006. Attribute-based encryption for fine-grained access control of encrypted data. *Proceedings of the ACM Conference on Computer and Communications Security*, 89–98.

[6] Cenk Gündoğan, Peter Kietzmann, Martine Lenders, Hauke Petersen, Thomas C. Schmidt, and Matthias Wählisch. 2018. NDN, CoAP, and MQTT: A Comparative Measurement Study in the IoT. In *Proceedings of the 5th ACM Conference on Information-Centric Networking* (Boston, Massachusetts) *(ICN '18)*. Association for Computing Machinery, New York, NY, USA, 159–171. https://doi.org/10.1145/3267955.3267967

[7] Jeremy Horwitz and Ben Lynn. 2002. Toward Hierarchical Identity-Based Encryption. In *Advances in Cryptology — EUROCRYPT 2002*, Lars R. Knudsen (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 466–481.

[8] Internet Engineering Task Force (IETF). 1981. *TRANSMISSION CONTROL PROTOCOL*. Technical Report. Internet Engineering Task Force (IETF).

[9] Internet Engineering Task Force (IETF). 2008. *The Transport Layer Security (TLS) Protocol Version 1.2*. Technical Report. Internet Engineering Task Force (IETF).

[10] Internet Engineering Task Force (IETF). 2011. *Extensible Messaging and Presence Protocol (XMPP): Core*. Technical Report. Internet Engineering Task Force (IETF).

[11] Internet Engineering Task Force (IETF). 2014. *The Constrained Application Protocol (CoAP)*. Technical Report. Internet Engineering Task Force (IETF).

[12] Internet Engineering Task Force (IETF). 2018. *The Transport Layer Security (TLS) Protocol Version 1.3*. Technical Report. Internet Engineering Task Force (IETF).

[13] S. P. Mathews and R. R. Gondkar. 2019. Protocol Recommendation for Message Encryption in MQTT. In *2019 International Conference on Data Science and Communication (IconDSC)*. 1–5.

[14] OASIS. 2014. *MQTT Version 3.1.1*. Technical Report. OASIS.

[15] OASIS. 2019. *MQTT Version 5.0*. Technical Report. OASIS.

[16] S. O'Dea. 2020. *Global industrial/consumer IoT connected objects 2018-2025. Statista Ltd.* Technical Report. https://www.statista.com/statistics/976079/number-of-iot-connected-objects-worldwide-by-type/

[17] Takeo Ogawara, Yoshihiro Kawahara, and Tohru Asami. 2013. Information dissemination performance of a disaster-tolerant NDN-based distributed application in disrupted cellular networks. In *IEEE P2P 2013 Proceedings*. 1–5. https://doi.org/10.1109/P2P.2013.6688722

[18] O. Sadio, I. Ngom, and C. Lishou. 2019. Lightweight Security Scheme for MQTT/MQTT-SN Protocol. In *2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*. 119–123.

[19] Jae Hong Seo and Keita Emura. 2015. Revocable Hierarchical Identity-Based Encryption: History-Free Update, Security Against Insiders, and Short Ciphertexts. In *Topics in Cryptology — CT-RSA 2015*, Kaisa Nyberg (Ed.). Springer International Publishing, Cham, 106–123.

[20] M. Singh, M. A. Rajan, V. L. Shivraj, and P. Balamuralidhar. 2015. Secure MQTT for Internet of Things (IoT). In *2015 Fifth International Conference on Communication Systems and Network Technologies*. 746–751.

[21] X. Wang, J. Zhang, E. M. Schooler, and M. Ion. 2014. Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT. In *2014 IEEE International Conference on Communications (ICC)*. 725–730.

[22] George Xylomenos, Christopher N. Ververidis, Vasilios A. Siris, Nikos Fotiou, Christos Tsilopoulos, Xenofon Vasilakos, Konstantinos V. Katsaros, and George C. Polyzos. 2014. A Survey of Information-Centric Networking Research. *IEEE Communications Surveys Tutorials* 16, 2 (2014), 1024–1049. https://doi.org/10.1109/SURV.2013.070813.00063

A CORRECTNESS ANALYSIS ON THE SIMULATION OF SUBSCRIPTION QUERY IN THE PROOF OF THEOREM 4.2

We first focus on the first term a_0 of the secret key for $PK_{Topic|k}$, since it contains the master secret key c_1^{α}, which is unknown to C. By setting the public parameters as shown in the proof of Theorem 4.2, we have

$$\begin{aligned} & h_1^{T_1} \ldots h_k^{T_k} \cdot c_2 \\ = \; & \prod_{i=1}^{k} (g^{\gamma_i} / y_{\ell-i+1})^{T_i} \cdot (g^{\delta} \cdot \prod_{i=1}^{\ell} y_{\ell-i+1}^{T_i^*}) \\ = \; & \left(g^{\delta+\sum_{i=1}^{k} T_i\gamma_i}\right) \cdot \left(\prod_{i=1}^{k} y_{\ell-i+1}^{-T_i}\right) \cdot \left(\prod_{i=1}^{\ell} y_{\ell-i+1}^{T_i^*}\right) \\ = \; & \left(g^{\delta+\sum_{i=1}^{k} T_i\gamma_i}\right) \cdot \left(\prod_{i=1}^{k} y_{\ell-i+1}^{T_i^*-T_i}\right) \cdot \left(\prod_{i=k+1}^{\ell} y_{\ell-i+1}^{T_i^*}\right) \end{aligned}$$

Note that the $\left(\prod_{i=1}^{k-1} y_{\ell-i+1}^{T_i^*-T_i}\right) = 0$ since $T_i = T_i^*$ for $i < k$. Thus,

$$h_1^{T_1} \ldots h_k^{T_k} \cdot c_2 = \left(g^{\delta+\sum_{i=1}^{k} T_i\gamma_i}\right) \cdot y_{\ell-k+1}^{T_k^*-T_k} \cdot \left(\prod_{i=k+1}^{\ell} y_{\ell-i+1}^{T_i^*}\right).$$

For simplicity, we denote $\left(g^{\delta+\sum_{i=1}^{k} T_i\gamma_i}\right) \cdot \left(\prod_{i=k+1}^{\ell} y_{\ell-i+1}^{T_i^*}\right)$ by X. By implicitly setting $r = \frac{\alpha^k}{(T_k - T_k^*)} + \tilde{r}$, we have that

$$\begin{aligned} (h_1^{T_1} \ldots h_k^{T_k} \cdot c_2)^r &= X^r \cdot (y_{\ell-k+1}^{T_k^*-T_k})^r \\ &= X^r \cdot (y_{\ell-k+1}^{T_k^*-T_k})^{\frac{\alpha^k}{(T_k-T_k^*)}+\tilde{r}} \\ &= X^r \cdot y_{\ell-k+1}^{-\alpha^k} \cdot y_{\ell-k+1}^{\tilde{r}(T_k^*-T_k)} \\ &= X^r \cdot y_{\ell+1}^{-1} \cdot y_{\ell-k+1}^{\tilde{r}(T_k^*-T_k)} \end{aligned}$$

Therefore, we have the secret key component

$$\begin{aligned} a_0 &= c_1^{\alpha} \cdot (h_1^{T_1} \ldots h_k^{T_k} \cdot c_2)^r \\ &= (y_{\ell+1} y_1^{\gamma}) \cdot X^r \cdot y_{\ell+1}^{-1} \cdot y_{\ell-k+1}^{\tilde{r}(T_k^*-T_k)} \\ &= y_1^{\gamma} \cdot X^r \cdot \cdot y_{\ell-k+1}^{\tilde{r}(T_k^*-T_k)}. \end{aligned}$$

Note that the term

$$X^r = \left[\left(g^{\delta+\sum_{i=1}^{k} T_i\gamma_i}\right) \cdot \left(\prod_{i=k+1}^{\ell} y_{\ell-i+1}^{T_i^*}\right)\right]^{\frac{\alpha^k}{(T_k-T_k^*)}+\tilde{r}}$$

can be easily computed by C using the knowledge of C and the instance of the ℓ-wBDHI problem, so as $a_1, b_{k+1}, \ldots, b_{\ell}$. Therefore, C can generate valid secret keys for $\mathcal{A}$ without the knowledge of $y_{\ell+1}$.