Enhancement of a Lightweight Attribute-Based Encryption Scheme for the Internet of Things

Syh-Yuan Tan, Kin-Woon Yeow, and Seong Oun Hwang, *Senior Member, IEEE*

***Abstract*—In this paper, we present the enhancement of a lightweight key-policy attribute-based encryption (KP-ABE) scheme designed for the Internet of Things (IoT). The KP-ABE scheme was claimed to achieve ciphertext indistinguishability under chosen-plaintext attack in the selective-set model but we show that the KP-ABE scheme is insecure even in the weaker security notion, namely, one-way encryption under the same attack and model. In particular, we show that an attacker can decrypt a ciphertext which does not satisfy the policy imposed on his decryption key. Subsequently, we propose an efficient fix to the KP-ABE scheme as well as extending it to be a hierarchical KP-ABE (H-KP-ABE) scheme that can support role delegation in IoT applications. An example of applying our H-KP-ABE on an IoT-connected healthcare system is given to highlight the benefit of the delegation feature. Lastly, using the NIST curves secp192k1 and secp256k1, we benchmark the fixed (hierarchical) KP-ABE scheme on an Android phone and the result shows that the scheme is still the fastest in the literature.**

***Index Terms*—Attribute-based, cryptanalysis, encryption, hierarchical, Internet of Things (IoT), key-policy, lightweight.**

I. Introduction

THE CONCEPT of identity-based encryption (IBE) scheme was first proposed by Shamir [32] in 1984 but the first concrete scheme was proposed 20 years later by Boneh and Franklin [6] with the help of bilinear pairing operation. IBE is proposed to eliminate the need of certification in public key infrastructure (PKI), where a user's public identity string, such as name, e-mail, phone number, national number, and so on is used as the user public key. There are only two entities in IBE, namely, the private key generator (PKG) and user. PKG generates users' decryption keys upon receiving the identities from users. When key generations are done, PKG can go offline and the users can communicate to each other in peer-to-peer (P2P) mode. Due to this key escrow property in PKG, IBE is suitable to be deployed in a closed system, such as that in Internet of Things (IoT) applications. For example, a factory can setup a PKG server to generate the decryption keys for each sensor, machine, IP camera, and smart phone with the MAC addresses or phone numbers as the public identities. The PKG server can then go offline and activates again only when it is necessary while the IoT devices can communicate securely in P2P mode.

Although IBE system is more efficient as compared to PKI, it remains a problem at the moment of selecting the most appropriate public identity as the public key. Sahai and Waters [30] are the first to answer this by extending IBE to support multiple identities which termed as attributes in their attribute-based encryption (ABE) scheme. In ABE, a decryption is successful if the attribute set ω on a ciphertext is close to the attribute set ω' on user decryption key for a predefined threshold t such that $|\omega \cap \omega'| \geq t$. ABE schemes blossom since then and further developed into key-policy ABE (KP-ABE) [16] and ciphertext-policy ABE (CP-ABE) [5] schemes. In KP-ABE scheme, an access policy $\mathbb{A}$ is imposed on the user decryption key and the decryption is successful only when the attribute set ω on ciphertext can satisfy the policy such that $\mathbb{A}(\omega) = \text{OK}$. For instance, an access policy on decryption key can be generated as $\mathbb{A} = \{10.0.0.123$ OR *MachineX* OR (*AdminHP* AND *SensorDept*)$\}$ so that the key can only decrypt the ciphertexts intended for either the IP address of 10.0.0.123, or *MachineX* or an administrator's smart phone from the sensor department. The CP-ABE scheme on the other hand places $\mathbb{A}$ on ciphertext and the concept of decryption is the reverse of KP-ABE scheme.

In order to deploy ABE schemes on IoT devices, some technical problems have to be addressed, such as the limitations of processing power, memory, and battery life. An ideal IoT-friendly ABE scheme needs to possess low algorithm complexity, short system parameters, short decryption key, and short ciphertext to cover these limitations yet remains secure at the same time. In view of this, KP-ABE schemes appears to be a better candidate compared to CP-ABE schemes because the former has faster encryption process in which the ciphertext only involves attribute tagging, instead of the generation of an access control policy. Besides, in general, an efficient ABE schemes can be constructed on elliptic curve (EC) [3]–[5], [15]–[19], [25], [26], [42], [45], [46] and Lattice [7]–[9] with the former possessing lightweight algorithms while the latter resisting quantum adversaries with higher algorithm complexity. Without considering the quantum adversaries, EC-based KP-ABE is a more appropriate candidate for IoT devices and

Manuscript received July 3, 2018; revised November 22, 2018 and February 16, 2019; accepted February 18, 2019. Date of publication February 25, 2019; date of current version July 31, 2019. This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIP) (No.2017R1A2B4001801). *(Corresponding author: Seong Oun Hwang.)*

S.-Y. Tan is with the School of Computing, Newcastle University, Newcastle upon Tyne NE4 5TG, U.K. (e-mail: syh-yuan.tan@newcastle.ac.uk).

K.-W. Yeow is with the Faculty of Electrical Engineering and Computer Science, Leibniz Universität, 30167 Hannover, Germany (e-mail: kinwoon@sim.uni-hannover.de).

S. O. Hwang is with the Department of Software and Communications Engineering, Hongik University, Sejong 30016, South Korea (e-mail: sohwang@hongik.ac.kr).

Digital Object Identifier 10.1109/JIOT.2019.2900631

we can further dissect the KP-ABE based on the types of EC. When a pairing-friendly curve is involved, a KP-ABE scheme needs to execute the costly bilinear pairing operation during decryption and this left us with pairing-free EC-based KP-ABE schemes as the best choice for IoT application.

However, provably secure pairing-free KP-ABE schemes are scarce. To the best of our knowledge, there are only two such schemes [18], [42] to-date. Herranz's provably secure pairing-free KP-ABE scheme [18] is widely recognized by the cryptographers to be the first of its kind. The KP-ABE scheme is based on ElGamal encryption scheme and achieves the ciphertext indistinguishability against chosen plaintext attack (IND-CPA) in the adaptive security model though it has a shortcoming in the performance. This is because its security parameters is linear to the number of maximum users supported and this resulted in huge public keys and ciphertext size. Also, it means that after the KP-ABE scheme is initialized, adding a new user to the system is not allowed unless the scheme is reset. Therefore, Herranz's KP-ABE scheme is a good candidate for one-time event that has small pool of users.

We discovered that, a year earlier than Herranz's work, Yao *et al.* [42] proposed an IND-CPA-secure pairing-free KP-ABE scheme in the selective security model, which is weaker than that of Herranz's but sufficient for IoT applications in the practice. Despite having the similar length in public parameters and user decryption keys compared to those of the state-of-the-art schemes, the KP-ABE scheme has approximately three times shorter ciphertext and two times lower computational overhead [42]. Although Yao *et al.*'s KP-ABE scheme cannot support heterogeneous IoT model yet, it has been selected as the core engine to secure the transaction of a billing system in vehicular cloud computing architecture [28] and to secure the health record transmission of a medical-cyber physical system [24]. The KP-ABE scheme was also referred in [13], [22], [29], [33], [44], and [47] but none of these works analyze its security in depth.

A. Contribution

In this paper, we cryptanalyze Yao *et al.*'s lightweight KP-ABE [42] scheme and discover a vulnerability in the key generation algorithm. Subsequently, we demonstrate that Yao *et al.*'s KP-ABE scheme is not even secure in the weaker security notion, namely, one-way encryption under chosen-plaintext attack (OWE-CPA) in the selective-set model. This indicates that a malicious user $\mathcal{A}$ can unauthorizedly decrypt a ciphertext whose attributes do not satisfy the policy on $\mathcal{A}$'s decryption key. As a result, we proposed an efficient fix for the vulnerability and also extend the fixed KP-ABE into a hierarchical KP-ABE (H-KP-ABE) scheme. The H-KP-ABE answers the open problem of poor generality [42] in the original scheme, where H-KP-ABE can simultaneously support unit IoT and ubiquitous IoT applications which require single PKG and multi-PKG, respectively.

B. Organization

This paper is organized as follows. We briefly describe the related mathematical tools and the security notions of KP-ABE scheme in Section II. The KP-ABE scheme proposed by Yao *et al.* is presented in Section III, followed by the cryptanalysis result in Section IV. In Section V, we present the efficient fix and also the H-KP-ABE scheme. Finally, we conclude this paper in Section VI.

II. Preliminaries

In this section, we briefly describe the mathematical assumption and tools needed to define the KP-ABE scheme and its security notions.

A. Lagrange Coefficient

In 1979, Shamir proposed the first secret sharing scheme [31], which applies the polynomial interpolation technique. It states that a n-degree polynomial can be reconstructed by computing $f_n(x) = \sum_{k=0}^{n} \Delta_{i,S}(x) y_i$ when $(n+1)$ points are given, where $\Delta_{i,S}$ is called the Lagrange coefficient.

Definition 1: Given that $(n+1)$ points represented by (x_i, y_i) for $i = \{0, \ldots, (n-1)\}$, $\Delta_{i,S}(x)$ can be computed as $\Delta_{i,S}(x) = \prod_{j=0, j\neq k}^{n} (x - x_j / x_k - x_j)$.

For sharing a secret a_0 among n number of parties and recovering with the presence of minimum t parties, a $(t-1)$-degree polynomial $f_{(t-1)}(x) = \sum_{i=0}^{t-1} a_i x^i \mod q$ is constructed, where, the coefficients $a_1, a_2, \ldots, a_{t-1} \in \mathbb{Z}_q^*$ are randomly selected. Each secret share $f(x)$ is equally distributed for i number of users. When t tuples $(x, f(x))$ are presented, the polynomial $f_{(t-1)}(x)$ can be reconstructed by Lagrange interpolation and the secret $f(0) = a_0$ is recovered.

B. Access Tree

Similar to Goyal *et al.*'s scheme [16], Yao *et al.*'s KP-ABE scheme [42] views access policy as an access tree as follows. Throughout this paper, we will use the symbol $\mathbb{A}$ to represent an access policy in the text form and Γ to represent an access policy in the mathematical form.

Definition 2 (Access Tree): Let Γ represents an access tree. Individually every nonleaf node of the access tree represents a threshold gate, that represented by its children and a threshold value. Let num_x be the number of children of the node x and d_x is its threshold value, then $0 < d_x \leq \text{num}_x$. When $d_x = 1$, the threshold gate is an OR gate, and when $d_x = \text{num}_x$, it is an AND gate. Each leaf node x of the access tree is described by an attribute and a threshold value $d_x = 1$.

The parent of node x in an access tree is denoted by $\text{parent}(x)$ and the function $\text{index}(x)$ returns the sequence number of node x under $\text{parent}(x)$, ranged from 1 to num_x. The index values can be uniquely assigned to nodes in the access tree for a given arbitrary key. The function $\text{attr}(x)$ is uniquely created for the leaf node x that represents the associated attribute. Γ_x is an access tree with root node x which returns 1 when it is satisfied by an attributes set ω such that $\Gamma_x(\omega) = 1$; otherwise, $\Gamma_x(\omega) = 0$. If x is a nonleaf node, $\Gamma_{x'}(\omega)$ is computed recursively for all its children x' and $\Gamma_x(\omega) = 1$ if and only if at least d_x children return 1. However, if x is a leaf node, $\Gamma_x(\omega) = 1$ if and only if $\text{attr}(x) \in \omega$.

C. KP-ABE Scheme

A KP-ABE scheme consists of four algorithms, namely, Setup, Encrypt, Key-Generation, and Decrypt [42].

1) *Setup (1^k):* Take in a security parameter and output the public key parameters Params and the master key MK.
2) *Encrypt (M, ω, Params):* Take in a message M, a set of attributes ω, and the public parameters Params to output the ciphertext CM.
3) *Key-Generation (Γ, MK, Params):* Take in an access tree Γ, the master key MK, and the public parameters Params as input to output the decryption key D corresponding to Γ.
4) *Decrypt (CM, D, Params):* Take the ciphertext CM, the decryption key D, and the public key parameters Params as input. If $\Gamma(\omega) = 1$, decrypt the ciphertext CM and output message M; otherwise, return $\perp$.

D. Security Model

The security notion of ciphertext IND-CPA in the selective-set model [16], [42] is defined as the game played between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as follows.

1) *Initialization:* The adversary $\mathcal{A}$ declares the set of attributes ω that it wishes to attack upon.
2) *Setup:* The challenger $\mathcal{C}$ runs the Setup algorithm and sends the public parameters Params to $\mathcal{A}$.
3) *Phase 1:* $\mathcal{A}$ is permitted to issue as many queries as it wants for the decryption keys for all access policy $\mathbb{A}_j$ such that $\mathbb{A}_j(\omega) = 0$, for all j.
4) *Challenge:* $\mathcal{A}$ submits two equal length messages M_0 and M_1 to $\mathcal{C}$. $\mathcal{C}$ flips a random coin v to encrypt M_v under the attributes set ω and return the ciphertext to $\mathcal{A}$.
5) *Phase 2:* Repeat Phase 1.
6) *Guess:* $\mathcal{A}$ outputs a guess v' of v.

A KP-ABE scheme is said to be IND-CPA secure in the selective-set model if $\mathcal{A}$ can win the game above with at most a negligible advantage $\epsilon = \Pr[v' = v] - (1/2)$ for all polynomial time adversary $\mathcal{A}$.

In the weaker security notion of OWE-CPA [34] in the selective-set model, the adversary $\mathcal{A}$ is given a ciphertext CM during the Challenge phase. $\mathcal{A}$ wins the game if the correct plaintext is recovered during the Guess phase such that $M = \text{Decrypt(CM)}$.

III. Yao *et al.*'s KP-ABE Scheme

We briefly describe Yao *et al.*'s KP-ABE [42] scheme before presenting the cryptanalysis result.

A. Setup (1^k)

Let $\mathbb{G}$ be a group of points on an EC with subgroup of prime order q defined over a finite field. Define the attribute universe as U, where $|U| = n$. For each attribute $i \in U$, choose a random $s_i \in \mathbb{Z}_q^*$ and the public key of each attribute i is $P_i = s_i G$, where $G \in \mathbb{G}$ is the base point. Next, choose a random $s \in \mathbb{Z}_q^*$ to be the master (private) key MK and the master public key PK is computed as $\text{PK} = sG$. The public parameters are denoted by $\text{Params} = \{\mathbb{G}, G, \text{PK}, P_1, \ldots, P_{|U|}\}$.

B. Encrypt (M, ω, Params)

To encrypt a message M under a set of attributes ω, randomly choose $k \in \mathbb{Z}_q^*$ to compute $C' = kPK = (K_x, K_y)$. Thereafter, compute $C_i = kP_i$ for each $i \in \omega$ and C and MAC_M as

$$C = \text{ENC}(M, K_x)$$
$$\text{MAC}_M = \text{HMAC}\big(M, K_y\big)$$

where $\text{ENC}(\cdot, \cdot)$ is a secure symmetric key encryption algorithm. The resulted ciphertext is denoted as $\text{CM} = (\omega, C, \text{MAC}_M, C_{i\in\omega})$.

C. Key-Generation (Γ, MK, Params)

Define a random polynomial $q_u(x)$ with degree of $(d_u - 1)$ for each node u in the access tree Γ in a top-down manner, where d_u is the threshold of the node u. For the root R of the access tree Γ, set $q_R(0) = s$ and choose $(d_R - 1)$ other points for the polynomial $q_R(x)$ randomly to determine it uniquely. For any other nodes (including leaf node) u, $q_u(0) = q_{\text{parent}(u)}(\text{index}(u))$. Similar to $q_R(x)$, $(d_u - 1)$ other points are chosen randomly to define polynomial $q_u(x)$.

When the polynomial of a leaf node u in the access tree is defined, a secret share of the decryption key for the leaf node u is defined as $D_u = (q_u(0)/s_i)$. This process is repeated for each leaf node and decryption key is defined as $D = \{D_u\} = \{(q_u(0)/s_i)\}$, where $i = \text{attr}(u)$ and $i \in \omega$.

D. Decrypt (CM, D, Params)

For each leaf node u, assuming $i = \text{attr}(u)$, the recursive procedure of decrypting each node $\text{DecryptNode(CM}, D, u)$ is defined as

$$\text{DecryptNode(CM}, D, u) = \begin{cases} D_u C_i = q_u(0) s_i^{-1} k P_i \\ \qquad\quad = q_u(0) s_i^{-1} k s_i G \\ \qquad\quad = q_u(0) k G, (i \in \omega) \\ \perp, \quad \text{Otherwise.} \end{cases}$$

For a nonleaf node u, call $\text{DecryptNode(CM}, D, v)$ for each of its child node v. Let S' be a set with arbitrary child nodes of u. For each node $v \in S'$, $\text{DecryptNode(CM}, D, v) \neq \perp$, produces a non-null output. If no such S' exists, $\text{DecryptNode(CM}, D, u) = \perp$. $\text{DecryptNode(CM}, D, u)$ is defined as follows, where $i = \text{index}(v)$ and $S = \{\text{index}(v), v \in S'\}$

$$\begin{aligned} &\text{DecryptNode(CM}, D, u) \\ &= \sum_{v\in S'} \Delta_{i,S}(0) \text{DecryptNode(CM}, D, v) \\ &= \sum_{v\in S'} \Delta_{i,S'}(0) q_v(0) kG \\ &= \sum_{v\in S'} \Delta_{i,S'}(0) q_{\text{parent}(v)}(\text{index}(v)) kG \\ &= \sum_{v\in S'} \Delta_{i,S'}(0) q_u(i) kG \\ &= q_u(0) kG. \end{aligned}$$

Based on DecryptNode(CM, D, R) $= q_R(0)(kG) = s(kG) = (K'_x, K'_y)$, the encrypted message M can be decrypted as $M' = \text{DEC}(C, K'_x)$ and verified such that $\text{HMAC}(M', K'_y) = \text{MAC}_M$.

IV. Cryptanalysis

In this section, we show that Yao *et al.*'s KP-ABE [42] scheme is insecure by mounting a chosen-plaintext attack (CPA) in the selective-set model to break the one-wayness of encryption. OWE-CPA is a weaker security notion compared to the IND-CPA claimed in [42]. The OWE-CPA presented here is an analogy of insider attackers $\mathcal{A}$ who can by-pass the access policy imposed on their decryption key to decrypt a prohibited ciphertext. In order to ease the explanation, we consider a small universe of attributes $U = \{x, y, z\}$ in which $\{x\}$ is the targeted attribute. Viewing x =9C:B6:54:49:C7:FA as the victim's MAC address, y = 10.0.0.1 and z = 10.0.0.2 as the IP addresses of malicious nodes obtained from Sybil attack, we show that the encrypted data of the victim can always be decrypted by the malicious nodes. Following the security model in Section II-D, the attack works as follows.

Initialization: $\mathcal{A}$ decided to attack the attribute $\omega = \{x\}$, i.e., decided to decrypt a ciphertext whose attribute is $\{x\}$.

Setup: $\mathcal{A}$ receives Params = $\{\text{PK}, P_x, P_y, P_z\}$.

Phase 1: $\mathcal{A}$ issues three queries for the decryption key with access policy $\mathbb{A}_1 = \{y \ \mathsf{OR} \ z\}$, $\mathbb{A}_2 = \{x \ \mathsf{AND} \ y\}$ and $\mathbb{A}_3 = \{x \ \mathsf{AND} \ y\}$, where $\mathbb{A}_2$ and $\mathbb{A}_3$ are the same attributes. Since $\mathbb{A}_1(\omega) = \mathbb{A}_2(\omega) = \mathbb{A}_3(\omega) = 0$, these decryption key queries are permitted according to the selective-set security model. In particular, the decryption keys are represented as $D_{\mathbb{A}_1} = \{D_y, D_z\}$, $D_{\mathbb{A}_2} = \{D_{u_x}, D_{u_y}\}$, and $D_{\mathbb{A}_3} = \{D'_{u_x}, D'_{u_y}\}$ such that

$$D_y = \frac{s}{s_y}$$

$$D_z = \frac{s}{s_z}$$

$$D_{u_x} = \frac{q_{u_x}(0)}{s_x} = \frac{q_{\text{root}}(\text{index}(x))}{s_x} = \frac{s + a(\text{index}(x))}{s_x}$$

$$D_{u_y} = \frac{q_{u_y}(0)}{s_y} = \frac{q_{\text{root}}(\text{index}(y))}{s_y} = \frac{s + a(\text{index}(y))}{s_y}$$

$$D'_{u_x} = \frac{q'_{u_x}(0)}{s_x} = \frac{q'_{\text{root}}(\text{index}(x))}{s_x} = \frac{s + a'(\text{index}(x))}{s_x}$$

$$D'_{u_y} = \frac{q'_{u_y}(0)}{s_y} = \frac{q'_{\text{root}}(\text{index}(y))}{s_y} = \frac{s + a'(\text{index}(y))}{s_y}$$

where the coefficients of root polynomial $a, a' \in \mathbb{Z}_q^*$ are randomly selected by PKG.

Challenge: $\mathcal{A}$ ends Phase 1 and receives the challenge ciphertext $\text{CM} = (\omega, C, \text{MAC}_M, C_1)$, where $C_1 = kP_1$, $\omega = \{x\}$, and $k \in \mathbb{Z}_q^*$.

Guess: $\mathcal{A}$ first extracts the valid decryption key D^* from $D_{\mathbb{A}_1}$, $D_{\mathbb{A}_2}$, and $D_{\mathbb{A}_3}$ as follows.

1) $X = (1/\text{index}(x))(D_{u_x} - D'_{u_x})$
$$= \frac{1}{\text{index}(x)}\left(\frac{s + a(\text{index}(x))}{s_x} - \frac{s + a'(\text{index}(x))}{s_x}\right)$$
$$= 1\left(\frac{s + a(1) - s - a'(1)}{s_x}\right)$$
$$= \frac{a - a'}{s_x}.$$

2) $Y = (1/\text{index}(y))(D_{u_y} - D'_{u_y})$
$$= \frac{1}{\text{index}(y)}\left(\frac{s + a(\text{index}(y))}{s_y} - \frac{s + a'(\text{index}(y))}{s_y}\right)$$
$$= \frac{1}{2}\left(\frac{s + a(2) - s - a'(2)}{s_y}\right)$$
$$= \frac{a - a'}{s_y}.$$

3) $D^* = X \times Y^{-1} \times D_y = (a - a'/s_x) \times (s_y/a - a') \times (s/s_y) = (s/s_x)$.

Chronologically, to successfully decrypt $M = \text{DEC}(C, K_x)$, $\mathcal{A}$ calculates C' as follows:

$$\begin{aligned} C' &= D^* \cdot C_1 \\ &= \frac{s}{s_x} kP_x \\ &= \frac{s}{s_x} ks_x P \\ &= ksP \\ &= kPK = \left(K_x, K_y\right). \end{aligned}$$

Since $\mathcal{A}$ can extract a valid decryption key for $\omega = \{x\}$, decryption is always successful. This shows that the one-wayness of Yao *et al.*'s KP-ABE scheme does not hold, where malicious users can collude together to generate a valid decryption key to decrypt a ciphertext which none of them alone can decrypt successfully.

A. Discussion

The main cause of the insecurity of Yao *et al.*'s KP-ABE scheme is in the key generation algorithm which is somehow deterministic, i.e., the decryption key are always the same if the access policy is a single level OR gate. Throughout the lifetime of the KP-ABE scheme, each attribute $i \in U$ is bound to a public parameter $P_i = s_i G$. Although the user decryption keys and their respective access policy are randomized using the random polynomials from secret sharing scheme, these polynomials are meant to converge and recover the master private key s. Thus, most of the randomness in the decryption keys can be eliminated also by applying the similar key recovery process.

One may question why this vulnerability exists while a security proof has been given by Yao *et al.* [42]. In order to answer this, we analyze the security proof and found that it is not correctly constructed. At the beginning of the proof, the simulator $\mathcal{B}$ was allowed to choose the scalar multipliers $c, d, z \in \mathbb{Z}_q^*$ and set them as the ECDDH challenge for $\mathcal{A}$. This allows $\mathcal{B}$ to set the shared secret in the root polynomial as $Q_R(0) = c$ during the key generation in Phase 1. Such setting is actually a wrong-doing as it violates the assumption of ECDDH, where the scalar multipliers of the elements in the ECDDH instance $(A, B, Z) = (cG, dG, cdG \text{ or } zG)$ should not be known to $\mathcal{B}$. If $\mathcal{B}$ knows c, deciding whether $Z = cdG$ or $Z = zG$ can be easily done by checking if $cB = Z$. In other words, even though finally the adversary $\mathcal{A}$ makes a correct guess $v' = v$ on M_v, $\mathcal{B}$ cannot use this information to break the ECDDH assumption simply because the assumption does not exist in the proof, and yields the security game meaningless.

V. Improvements

In order to prevent the CPA attack, we have to slightly modify the definition of index(·) function in Section II-B by using an extra pseudorandom number generator PRF : $\{0,1\}^k \times \{0,1\}^* \to \mathbb{Z}_q^*$. In particular, we replace the function index(·) by a new function index(·)′ = PRF(r, index(·)) which generates sequence numbers based on a random salt r of k bits together with the output of index(·). This increases the decryption key size with extra $k \times n$ bits, where k is the PRF algorithm block size and n is the total hierarchy level. For example, $k = 512$ if the HMAC-SHA256 algorithm is used; $k = 1024$ if the HMAC-SHA384 and HMAC-SHA512 are used. For instance, the sequence numbers of $D_{\mathbb{A}_2}$ and $D_{\mathbb{A}_3}$ in our CPA attack can be computed as follows:

$$
\begin{aligned}
D_{u_x} &= \frac{q_{u_x}(0)}{s_x} = \frac{q_{\text{root}}\big(\text{index}(x)'\big)}{s_x} \\
&= \frac{q_{\text{root}}\big(\text{PRF}\big(r_{\mathbb{A}_2}, \text{index}(x)\big)\big)}{s_x} = \frac{s + a\big(\text{PRF}\big(r_{\mathbb{A}_2}, 1\big)\big)}{s_x} \\
D_{u_y} &= \frac{q_{u_y}(0)}{s_y} = \frac{q_{\text{root}}\big(\text{index}(y)'\big)}{s_y} \\
&= \frac{q_{\text{root}}\big(\text{PRF}\big(r_{\mathbb{A}_2}, \text{index}(y)\big)\big)}{s_y} = \frac{s + a(\text{PRF}(r_{\mathbb{A}_2}, 2))}{s_y} \\
D'_{u_x} &= \frac{q'_{u_x}(0)}{s_x} = \frac{q'_{\text{root}}\big(\text{index}(x)'\big)}{s_x} \\
&= \frac{q'_{\text{root}}\big(\text{PRF}\big(r_{\mathbb{A}_3}, \text{index}(x)\big)\big)}{s_x} = \frac{s + a'\big(\text{PRF}(r_{\mathbb{A}_3}, 1)\big)}{s_x} \\
D'_{u_y} &= \frac{q'_{u_y}(0)}{s_y} = \frac{q'_{\text{root}}\big(\text{index}(y)'\big)}{s_y} \\
&= \frac{q'_{\text{root}}\big(\text{PRF}\big(r_{\mathbb{A}_3}, \text{index}(y)\big)\big)}{s_y} = \frac{s + a'\big(\text{PRF}(r_{\mathbb{A}_3}, 2)\big)}{s_y}.
\end{aligned}
$$

Since the index(·)′ values in $D_{\mathbb{A}_2}$ and $D_{\mathbb{A}_3}$ are different now, the sequence numbers cannot be removed to forge the decryption key D^* as in the CPA attack. We emphasize that this is the only changes needed to prevent the CPA attack, and other algorithms in Yao *et al.*'s KP-ABE scheme can remain unchanged.

A. Security Proof

We make use of the modified decisional game from [5] to devise a security proof in the generic model for the fixed KP-ABE scheme. Instead of asking the adversary to decide whether the challenge ciphertext is either $C = \text{ENC}(M_0, K_x), \text{MAC}_M = \text{HMAC}(M_0, K_y)$ or $C = \text{ENC}(M_1, K_x), \text{MAC}_M = \text{HMAC}(M_1, K_y)$, we ask the adversary to decide either C and MAC_M are formed by using K_x, K_y or two random values $\alpha, \beta \in \mathbb{Z}_q$. We consider a random encoding ϕ of additive group $\mathbb{Z}_q$ such that $\phi : \mathbb{Z}_q \to \{0,1\}^n$, where $n > 3\lg(q)$. We are given an oracle to compute the induced group action on $\mathbb{G} : \{\phi(x) : x \in \mathbb{Z}_q\}$. We refer to $\mathbb{G}$ as a generic group. The following theorem gives a lower bound on the advantage of a generic adversary in breaking the fixed KP-ABE scheme.

Theorem 1: Let ENC, MAC_M, and PRF be a secure symmetric encryption scheme, a secure message authentication code and a secure pseudorandom number generator, respectively, and let $\phi, \mathbb{G}$ be defined as above. For any adversary $\mathcal{A}$ for the fixed KP-ABE scheme, let q_e be a bound on the total number of group elements it receives from queries made to the key-generation oracle and from the interactions in the IND-CPA security game. The advantage of $\mathcal{A}$ in the IND-CPA security game is then $O(q_e/q)$.

Proof: Setting $G = \phi(1)$, we show that if an EC group can be modeled by a generic group, then the fixed KP-ABE scheme is secure against ciphertext indistinguishability under CPA by an adversary $\mathcal{A}$.

Initialization: $\mathcal{A}$ declares the set of attributes ω which will appear in the challenge ciphertext.

Setup: The simulation chooses random $s, s_i \in \mathbb{Z}_q^*$ to compute $\text{PK} = \phi(s)$ and $P_i = \phi(s_i)$ for $i \in U$. The public parameters $\text{Params} = \{\mathbb{G}, G, \text{PK}, P_1, \ldots, P_{|U|}\}$ are sent to $\mathcal{A}$.

Phase 1: When $\mathcal{A}$ issues queries for a decryption key for the access tree Γ, the simulator computes $D = \{D_u\}$ as in the fixed key-generation algorithm in Section V. In precise, for the root R, setting $q_R(0) = s$, the simulator chooses random coefficients $\lambda_j \in \mathbb{Z}_q^*$ and random strings $r_l \in \{0,1\}^k$ to construct the random $(d_R - 1)$-degree polynomial $q_R(\text{index}'(x))$, where $1 \le j \le d_R - 1$ and l range from 1 to the maximum hierarchy level in Γ. Note that $\text{index}'(x) \in \mathbb{Z}_q^*$ is a random value obtained from the PRF oracle using r_l and index(x) as the seed. For other nodes u, the simulator constructs the random polynomial $q_u(\text{index}'(u))$ similarly. In the case, where $\mathcal{A}$ asks for a decryption key for a Γ that can be satisfied by ω, the simulator aborts.

Challenge: When $\mathcal{A}$ submits the challenge messages M^* and the attribute set ω, the simulator randomly chooses $k \in \mathbb{Z}_q^*$ to compute $C_i = \phi(ks_i)$ for $i \in \omega$. The simulator then flips a random coin $b \in \{0,1\}$. If $b = 0$, the simulator randomly selects $\alpha, \beta \in \mathbb{Z}_q^*$ to compute C, MAC_{M^*}, where $K_x = \alpha, K_y = \beta$. Else $b = 1$, the simulator computes $C' = kPK = (K_x, K_y) = \phi(ks)$ and subsequently the values C, MAC_{M^*}. These values are passed to $\mathcal{A}$ as the challenge ciphertext.

Phase 2: $\mathcal{A}$ continues to issue new queries as in Phase 1 and the simulator replies as above.

Guess: $\mathcal{A}$ outputs a correct guess b' to indicate the ciphertext is proper encryption or not.

We now left with the probability calculation of $\mathcal{A}$ making a correct guess. As the simulation is perfect from $\mathcal{A}$'s view, there is no game abortion except the collision of elements mapping from ϕ with a probability of $1/|\mathbb{Z}_q^*| = 1/q$. Therefore, the lower bound of $\mathcal{A}$'s advantage in correctly guessing the ciphertext is $O(q_e/q)$ as claimed, where q_e is the total queries to ϕ. ■

B. Hierarchical KP-ABE

The fixed KP-ABE scheme can be extended into an H-KP-ABE by adopting the decryption key delegation techniques from [16]. With the more powerful H-KP-ABE, users can perform role delegation or even possible to achieve the on-the-fly

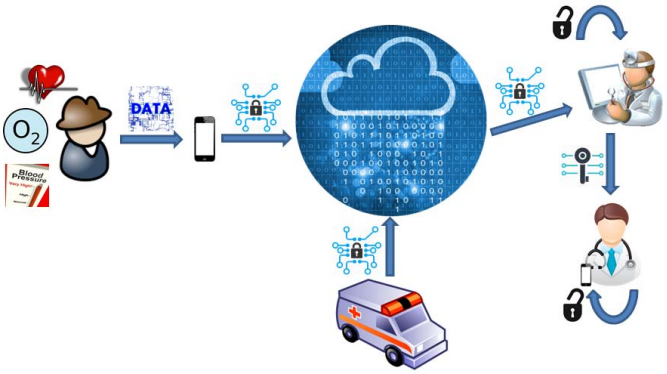


Fig. 1. IoT-connected Healthcare system.

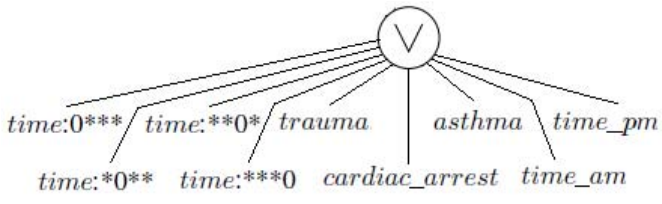


Fig. 2. Access policy on Dr. A's decryption key.

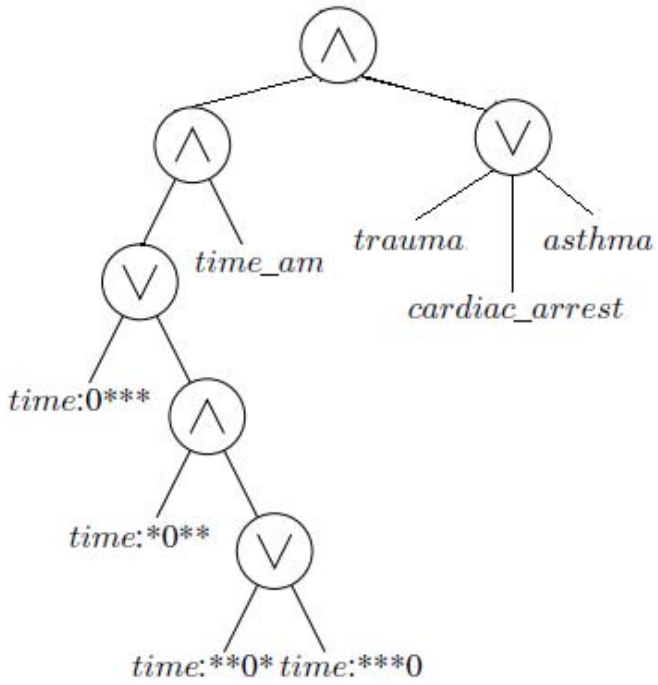


Fig. 3. Access policy on Dr. A's delegated decryption key.

P2P system [36]. The on-the-fly P2P system can be established by one or more PKGs (attribute authorities) with a designated objective and a finite duration which initially generate decryption keys to the new (level 1) users of the network. When the size of the system grows, a level 1 user is now promoted to be the sub-PKG. The sub-PKG can setup its own P2P group (level 2 users) but it can only generate decryption keys which are at most as strong as its own private key.

Considering the scenario of an IoT-connected healthcare system as depicted in Fig. 1, the proposed H-KP-ABE can be deployed to secure the communication between hospitals and the wearable medical system [38], [41] as well as the emergency medical system [39]. For an example, on 8 A.M., when the medical officer on ambulance completed the diagnosis on a patient, the data can be encrypted using the attributes {time : $1 * **$, time : $* 0 * *$, time : $* *0*$, time : $* * * 0$, time_am, cardiac_arrest, myocardial_infarction, stroke} and sent to the healthcare system, where the first five attributes represent 8 A.M. in binary format. The system then alerts the specialist on duty, Dr. A on the patient's arrival. We assume Dr. A's decryption key consists of the policy $\mathsf{ANY}(1)$(cardiac_arrest, trauma, asthma, time : $0***$, time : $*0**$, time : $**0*$, time : $***0$, time_am, time_pm) as depicted by Fig. 2.

If Dr. A is currently occupied, in order to delegate his patients to Dr. B, he can use H-KP-ABE to delegate the patient's data to Dr. B in a P2P manner, i.e., without contacting the PKG. There are a few advantages of delegation feature in H-KP-ABE compared to the naive delegation mechanism in KP-ABE in which Dr. A has to decrypt the patient data and re-encrypt it under Dr. B's public key. First, H-KP-ABE is significantly more efficient compared to KP-ABE in terms of role delegation as Dr. A only needs to generate a subkey as the delegated decryption key, instead of performing both encryption and decryption. Second, H-KP-ABE allows Dr. A to achieve fine-grained control on the delegated decryption key while KP-ABE cannot. For instance, Dr. A wishes to take over his own patients after 11 A.M. He can pass to Dr. B a delegated decryption key which is valid until 11 A.M. only. The stricter access policy can be designed as $\mathsf{AND}(\mathsf{AND}(\mathsf{OR}(\text{time} : 0 * **, \mathsf{AND}(\text{time} : * 0 * *, \mathsf{OR}(\text{time} : * *0*, \text{time} : * * * 0))), \text{time\_am}), \mathsf{ANY}(1)(\text{cardiac\_arrest}, \text{trauma}, \text{asthma}))$ as shown in Fig. 3. The left branch allows the checking of <11 by comparing the bits location of Dr. B's decryption time.

The generation of such delegated decryption key be done by running the following algorithm, where l is the additional threshold to be added.

1) Subkey-Generation (Γ, D, *Params):* Define a new degree value $d'_u = d_u + l$ for each node u in the access tree Γ in a top-down manner, where $d'_u \leq n$ and n is the total number of nodes at the same level. For each polynomial $q_u(x)$ in Γ whose new degree d'_u is determined, define the new polynomial as $q_u(x)' = q_u(x)(x+1)^l$, where $x = \text{index}(\cdot)'$.

When the polynomial of a leaf node u in the access tree is defined, a secret share of the decryption key for the leaf node u is defined as $D'_u = D_u(x+1)^l = [(q_u(0)(x+1)^l)/s_i]$. This process is repeated for each leaf node and decryption key is defined as $D' = \{D'_u\} = \{[(q_u(0)(x+1)^l)/s_i]\}$, where $i = \text{attr}(u)$ and $i \in \omega$.

Remark: The new threshold value $t' = t+l$ cannot be greater than the total leaf nodes n such that $t' \leq n$. Referring to the toy example, Dr. A's key policy $\mathsf{ANY}(1)$ is a $(1, 9)$-threshold gate and the policy in the new decryption key created by him can be at most a $(9,\ 9)$-threshold gate, which is an AND of all attributes.

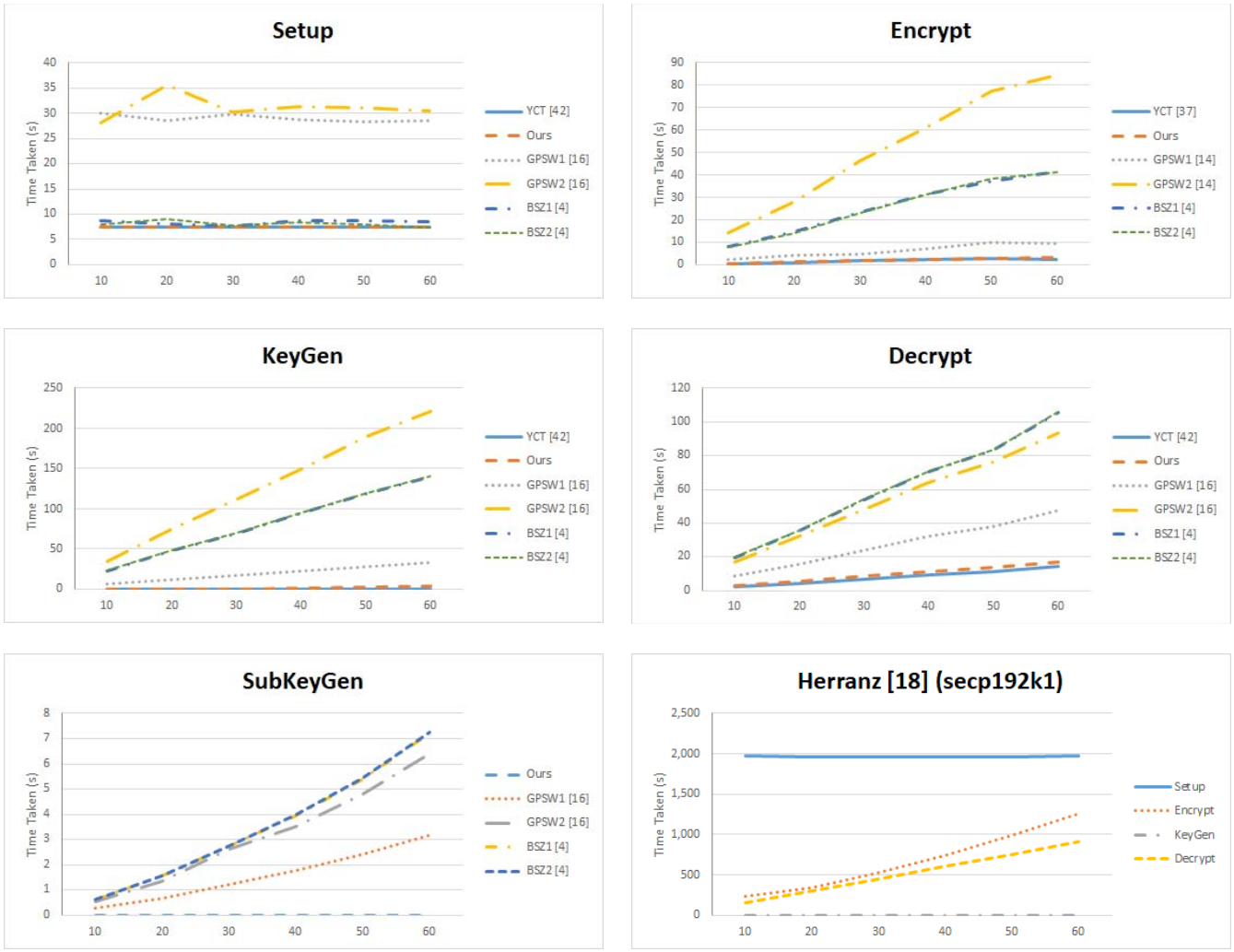


Fig. 4. Performance of H-KP-ABE at 80-bit security on phone.

The following theorem claims the security of the H-KP-ABE scheme.

Theorem 2: Let ENC, MAC_M, PRF be a secure symmetric encryption scheme, a secure message authentication code and a secure pseudorandom number generator, respectively, and let $\phi, \mathbb{G}$ be defined as above. For any adversary $\mathcal{A}$ for the H-KP-ABE scheme, let q_e be a bound on the total number of group elements it receives from queries made to the key-generation and subkey-generation oracles, as well as from the interactions in the IND-CPA security game. The advantage of $\mathcal{A}$ in the IND-CPA security game is then $O(q_e/q)$.

Proof: The proof is similar to that in Theorem 1 with the simulation of an additional subkey-generation oracle, whose operations can be extracted from the key-generation oracle. ■

C. Comparison and Analysis

The original Yao *et al.*'s KP-ABE scheme together with several other ABE schemes have been benchmarked in [47] on PC with processor i7-4710HQ (3.4 GHz) under the Charm framework [1] which is written in C language. Using the access policy of $\mathsf{AND}(\text{attr}_3, \mathsf{OR}(\text{attri}_1, \text{attr}_2))$, Yao *et al.*'s KeyGen and Decrypt can be completed in 0.161 and 0.557 s, respectively; while other ABE schemes need at least 1.733 and 0.559 s, or the maximum 49.184 and 3.322 s, respectively. This shows that the original Yao *et al.*'s KP-ABE scheme is the most efficient ABE scheme in the literature, where it is at least ten times faster than normal ABE schemes. We are interested to know whether the strength in efficiency still hold when the security fix is applied.

In this section, we benchmark the original Yao *et al.*'s KP-ABE scheme and the fixed scheme in: 1) an Android phone which runs Android 4.4.2 with 2GB RAM on Quad-core 2.3 GHz Krait 400 processor and 2) an end user PC which runs Windows 7 Pro 64-bit with 4 GB RAM on Intel i3-2120s 3.3 GHz processor. The schemes are implemented using Java cryptography extension and the ECC library optimized for Android from [35].

First, we quantify the efficiency loss due to the security fix of KP-ABE scheme on Android phone to mimic the environment of an IoT device. Two ECs are chosen, namely, secp192k1 and secp256k1 which provides 80-bit and 128-bit security, respectively. AES-128 and HMAC-SHA256 are selected to represent the secure symmetric

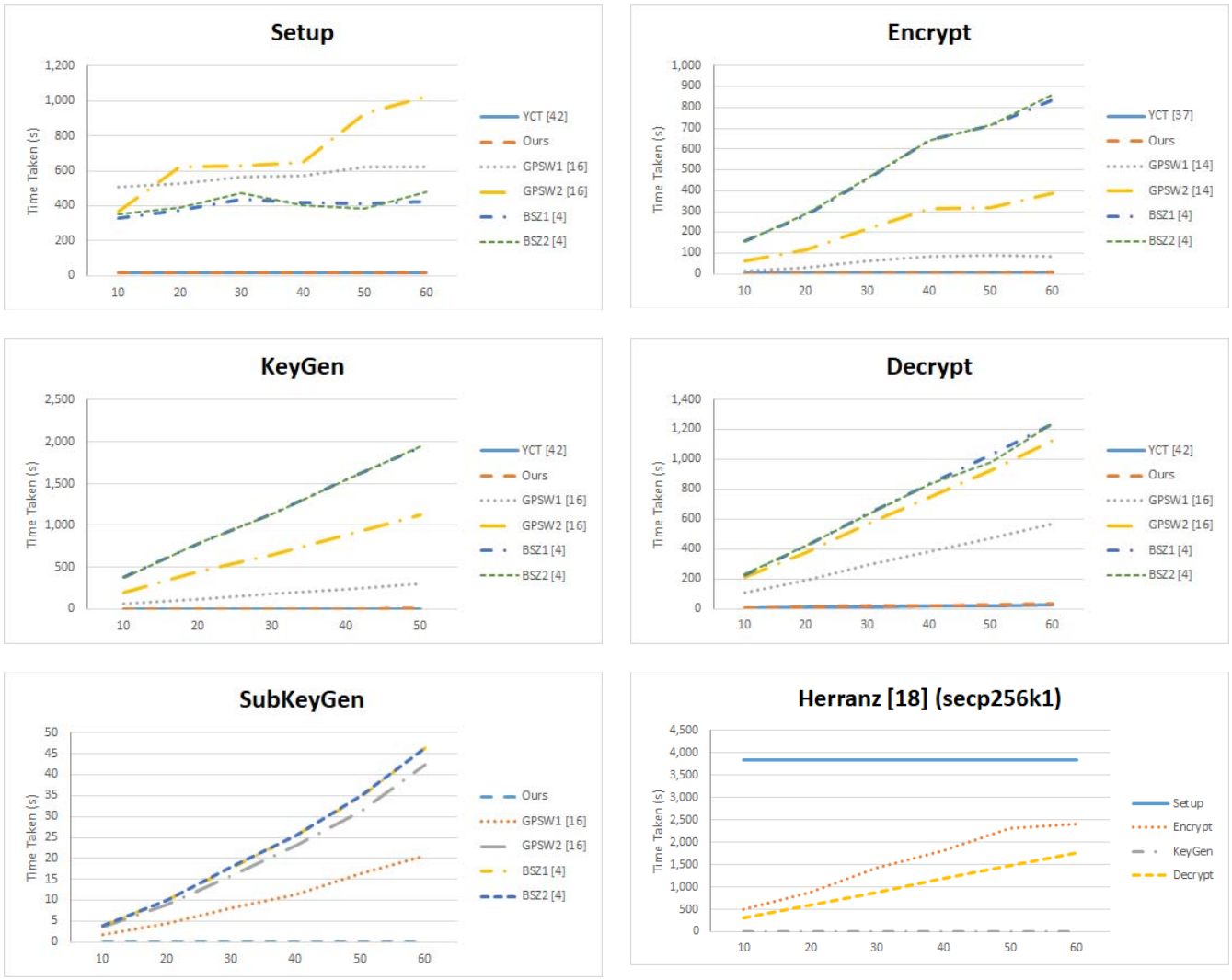


Fig. 5. Performance of H-KP-ABE at 128-bit security on phone.

TABLE I
PERFORMANCE OF YAO *et al.*'S KP-ABE SCHEME ON PHONE (UNIT: MILLISECOND)

	80-bit security (secp192k1)	128-bit security (secp256k1)
Setup	10,305.38	13,119.03
Encrypt	351.08	906.96
KeyGen	5.39	5.54
Decrypt	1,656.60	2,370.36

TABLE II
PERFORMANCE OF FIXED KP-ABE SCHEME ON PHONE (UNIT: MILLISECOND)

	80-bit security (secp192k1)	128-bit security (secp256k1)
Setup	10,389.05	13,507.82
Encrypt	378.19	891.85
KeyGen	7.04	7.71
Decrypt	1,956.91	2,847.49

key encryption algorithm and MAC algorithm in encrypt. Furthermore, the plaintext of the scheme is set as a random 1024 bits message and we fix the same ten random attributes $(\text{attr}_1, \text{attr}_2, \ldots, \text{attr}_{10})$ during Encrypt and KeyGen with the access policy $\mathsf{AND}(\text{attr}_1, \text{attr}_2, \ldots, \text{attr}_{10})$. The algorithms are run for 1100 rounds with the first 100 rounds omitted and the average timing in milliseconds of the remaining 1000 rounds are recorded.

From Tables I and II, notice that the performance of Encrypt algorithm are about the same. This is because our security fix modifies the index(x) function in KeyGen and Decrypt algorithms only. However, KeyGen of our improved scheme is decelerated for approximately 23% under secp192k1 and 28% under secp256k1; while the Decrypt is 15% slower under secp192k1 and 17% slower under secp256k1. Even though the performance of decryption is slightly decreased, the fixed scheme is still the fastest in the literature as shown in Figs. 4–7.

We also compare the proposed H-KP-ABE to four state-of-the-art pairing-based KP-ABE schemes [4], [16] and a pairing-free KP-ABE scheme [18]. First, we extend Baek *et al.*'s and Goyal *et al.*'s KP-ABE schemes into

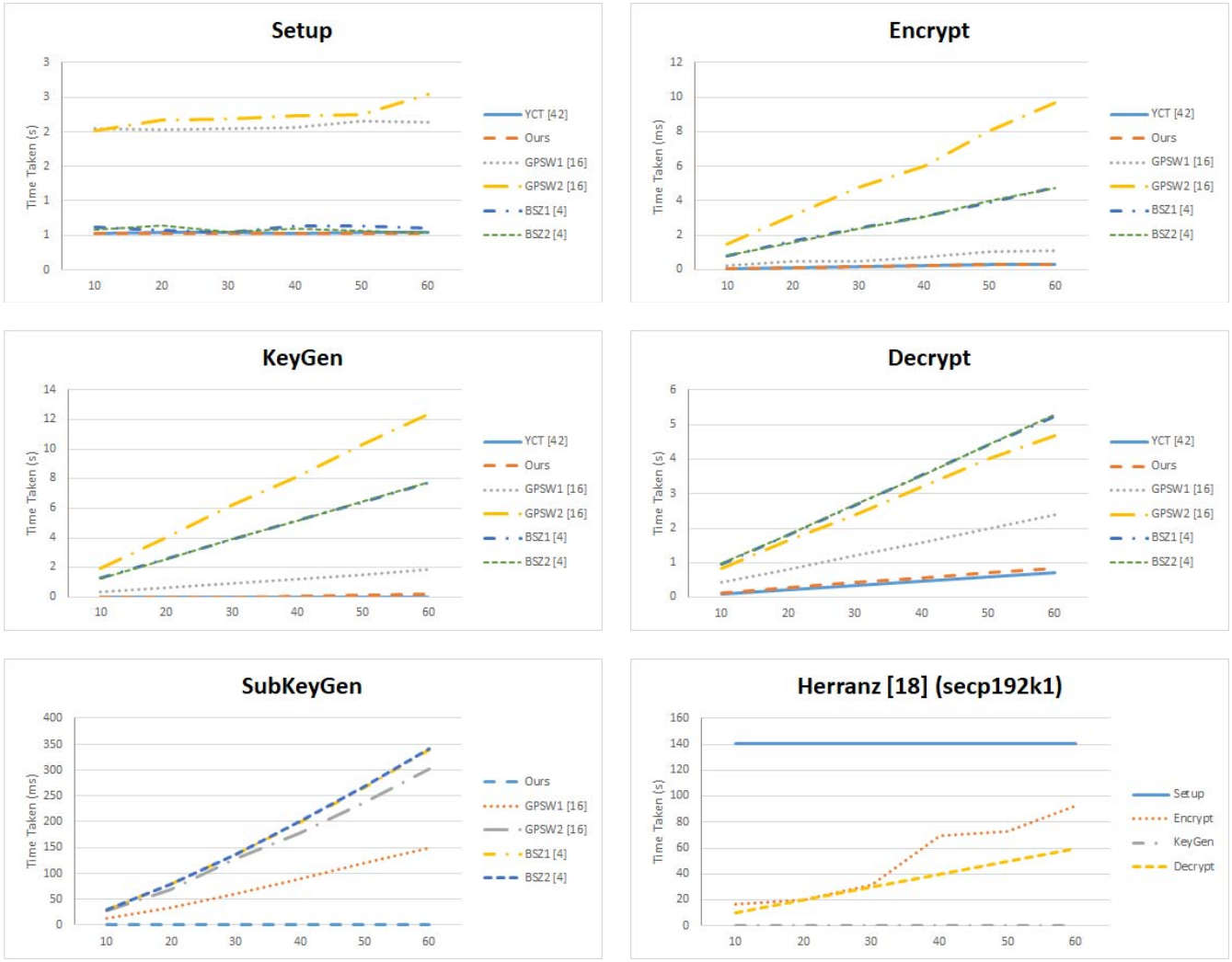


Fig. 6. Performance of H-KP-ABE at 80-bit security on PC.

H-KP-ABE using the technique described in Section V-B. Next, we run the four H-KP-ABE schemes on Type A curve [10] using 160-bit prime order with 1024-bit prime p for 80-bit security, and 256-bit prime order with 1536-bit prime p for 128-bit security. On the other hand, Herranz's KP-ABE is run on secp192k1 and secp256k1 since it does not require any pairing operation. We also set its user limit to 100, which is a part of its security parameter [18]. Although Herranz's KP-ABE scheme cannot be extended hierarchically, we still include it into the comparison as it is the only secure pairing-free KP-ABE that we know to-date besides Yao *et al.*'s.

We initialize the schemes with a total of 100 attributes as the attribute universe U, and set the number of attributes ω in the six sample ciphertexts as 10, 20, 30, 40, 50, and 60. Next, we craft six versions of access policies in the corresponding decryption key as (7, 10)-threshold gate [i.e., $\mathsf{ANY}(7)\{\text{attr}_1, \text{attr}_2, \ldots, \text{attr}_{10}\}$], (14, 20)-threshold gate, (21, 30)-threshold gate, (28, 40)-threshold gate, (35, 50)-threshold gate, and (42, 60)-threshold gate. For H-KP-ABE, we evaluate SubKeyGen for each access policy above by increasing threshold t to $t+3$. We illustrate the benchmarking results from phone in Figs. 4 and 5 while PC in Figs. 6 and 7.

At the first glance, in both platforms, the timing patterns of the (H-)KP-ABE schemes are not affected by the types of ECC curve. Yao *et al.*'s and our H-KP-ABE schemes appeared to be the fastest among all in every algorithm. Notice that under 128-bit security in the phone, our Setup algorithm can be completed within 15 s with $|U| = 100$; while KeyGen algorithm can be done within 6 s with $|\omega| = 60$. This is quite efficient given the fact that the former is only executed once per system life time while the latter is executed once for each user. In the case they are executed by PC, approximately 1 s is needed as shown in Figs. 6 and 7.

Besides, our H-KP-ABE encryption on phone exceeds 2 s when a ciphertext has more than 30 attributes. The corresponding decryption time is also linear to the number of attributes due to the polynomial interpolation operations. However, we argue that in practice one may not need that much of attributes to encrypt/decrypt a data as we can optimize the attributes assignment by grouping the attributes of same nature into a single attribute. For instance, instead of using 28 attributes month : 0∗∗∗, . . . , month : ∗∗∗0, month : 1∗∗∗, . . . , month : ∗∗∗1,day : 0∗∗∗∗, . . . , day : ∗∗∗∗0, day : 1∗∗∗∗, . . . , day : ∗∗∗∗1, time : 0∗∗∗, . . . , time : ∗∗∗0, time : 1∗∗∗, . . . , time : ∗∗∗1, time_am, time_pm to represent month, day

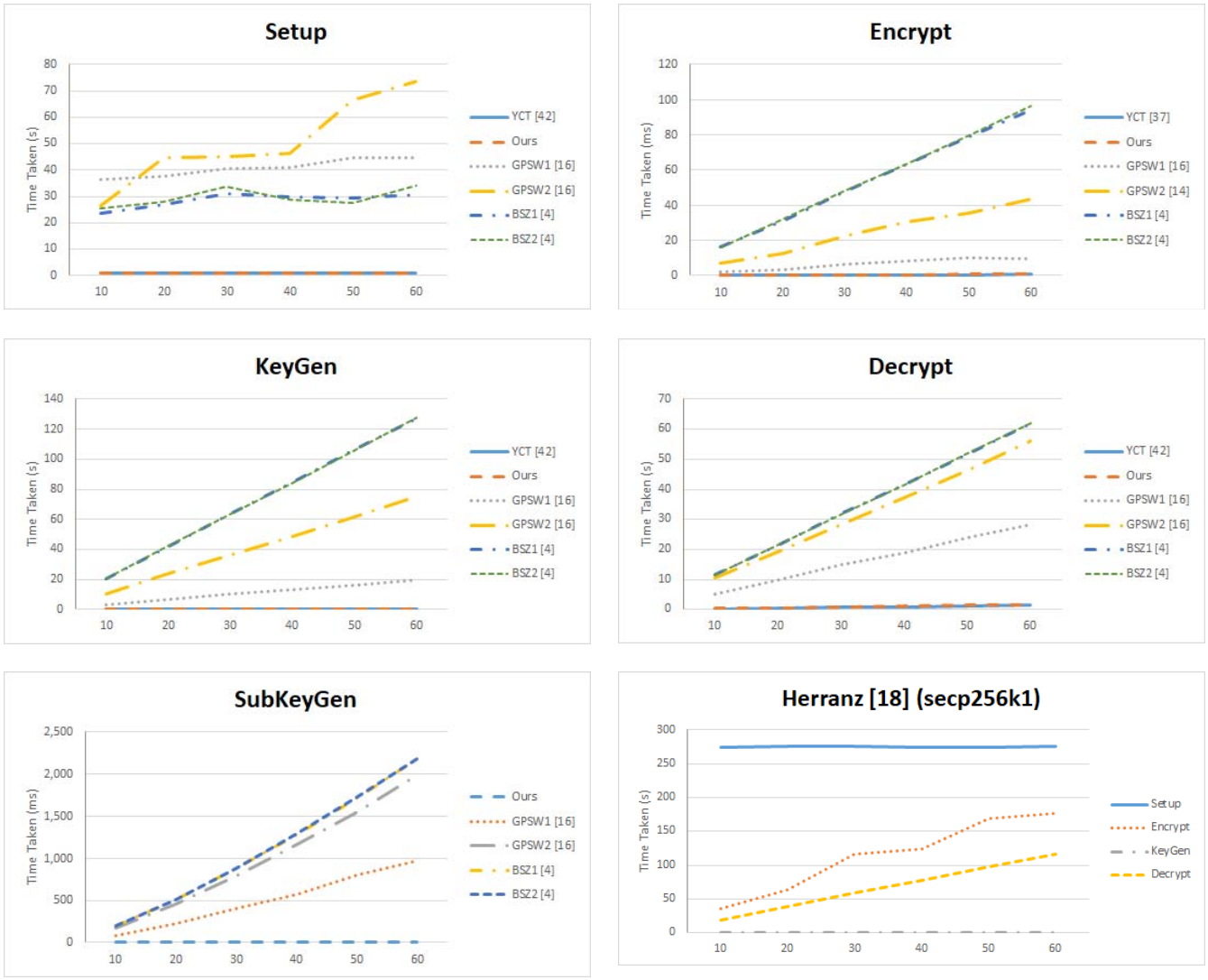


Fig. 7. Performance of H-KP-ABE at 128-bit security on PC.

and time, we can compress them to 13 attributes month, day, time, $1 * * * *, \ldots, * * * * 1, 0 * * * *, \ldots, * * * * *0$, where the binary attributes can AND with any of the first three attributes. If exact timing is not required in practice, attributes, such as ****1 and ****0 can be omitted to further reduce the polynomial degree and hierarchy level. Moreover, in the scenario, such as the smart factory [37], smart rehabilitation [14], and smart medical [38], [39], [41] whose IoT devices send data most of the times and take commands from server occasionally, decryption is frequently done by PC instead of IoT devices. In such applications, for ciphertext with 30 attributes, decryption can be completed within 0.5 and 0.9 s on secp192k1 and secp256k1, respectively, as shown in Figs. 6 and 7.

It is obvious that the pairing-based H-KP-ABE schemes are slower than our pairing-free H-KP-ABE scheme, though some of them like GPSW1, BSZ1, and BZS2 do not need to define the attribute universe before running the Setup algorithm. However, it is a common practice to identify the attributes in a system before setting it up and so this property is not a must. In fact, schemes like GPSW1 and ours which require the attribute universe to be established in advance are always more efficient, but Herranz's KP-ABE is an exception. We are surprised to see that the pairing-free KP-ABE scheme is the slowest in general. Out of the five algorithms, Herranz's KeyGen algorithm is the only algorithm which is faster than ours, when the number of attributes is greater than 30. Its poor performance is justifiable if we take into consideration the security level. Herranz's KP-ABE is proven secure in a stringent security model, namely, standard model with adaptive security that is stronger than the standard model with selective security adopted by GPSW1 and GPSW2 KP-ABE schemes. We think that sacrificing the performance and the useful delegation features in an efficient H-KP-ABE scheme in exchange to a stronger security assurance of a KP-ABE scheme is not a practical choice. Furthermore, there is an evidence [23] showing that the cryptographic schemes proven secure in the standard model are not necessarily more secure than those not proven so in the practice. Therefore, we believe our H-KP-ABE scheme is the optimum solution for IoT application and

we leave the design of the security proof in a stronger security model for our H-KP-ABE scheme as an open problem.

VI. Conclusion

We cryptanalyzed a pairing-free KP-ABE scheme designed for IoT applications. Subsequently, an efficient fix is proposed to secure against the discovered vulnerability and a hierarchical version is proposed to cover the scenario of decentralized P2P applications. Our benchmarking results suggest that the proposed H-KP-ABE scheme is suitable for IoT applications which perform encryption and role delegation on low powered devices but decryption on the server.

References

[1] J. A. Akinyele *et al.*, "Charm: A framework for rapidly prototyping cryptosystems," *J. Cryptograph. Eng.*, vol. 3, no. 2, pp. 111–128, 2013.

[2] L. M. Aiello, M. Milanesio, G. Ruffo, and R. Schifanella, "An identity-based approach to secure P2P applications with Likir," *Peer-to-Peer Netw. Appl.*, vol. 4, no. 4, pp. 420–438, 2011.

[3] N. Attrapadung *et al.*, "Attribute-based encryption schemes with constant-size ciphertexts," *Theor. Comput. Sci.*, vol. 422, pp. 15–38, Mar. 2012.

[4] J. Baek, W. Susilo, and J. Zhou, "New constructions of fuzzy identity-based encryption," in *Proc. ASIACCS 2nd ACM Symp. Inf. Comput. Commun. Security*, Singapore, 2007, pp. 368–370.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Security Privacy (SP)*, Berkeley, CA, USA, 2007, pp. 321–334.

[6] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 2001, pp. 213–229.

[7] D. Boneh *et al.*, "Fully key-homomorphic encryption arithmetic circuit ABE and compact garbled circuits," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2014, pp. 533–556.

[8] X. Boyen and Q. Li, "Turing machines with shortcuts: Efficient attribute-based encryption for bounded functions," in *Proc. 14th Int. Conf. Appl. Cryptography Netw. Security (ACNS)*, Guildford, U.K., 2016, Jun. pp. 19–22.

[9] X. Boyen and Q. Li, "Attribute-based encryption for finite automata from LWE," in *Proc. 9th Int. Conf. Provable Security (ProvSec)*, Kanazawa, Japan, 2015, pp. 247–267.

[10] X. Boyen and L. Martin, "Identity-based cryptography standard (IBCS) #1: Supersingular curve implementations of the BF and BB1 cryptosystems," Internet Eng. Task Force, Fremont, CA, USA, RFC 5091, 2007.

[11] K. R. B. Butler, S. Ryu, P. Traynor, and P. D. McDaniel, "Leveraging identity-based cryptography for node ID assignment in structured P2P systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 12, pp. 1803–1815, Dec. 2009.

[12] A. De Caro and V. Iovino, "jPBC: Java pairing based cryptography," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, 2011, pp. 850–855.

[13] K. Cooper, "Security for the Internet of Things," M.S. thesis, School Comput. Sci. Commun., KTH Roy. Inst. Technol., Stockholm, Sweden, 2015.

[14] Y. J. Fan, Y. H. Yin, L. D. Xu, Y. Zeng, and F. Wu, "IoT-based smart rehabilitation system," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1568–1577, May 2014.

[15] T. Feng, X. Yin, and C. Liu, "An efficient and anonymous KP-ABE scheme with keyword search," *Proc. Int. Conf. Inf. Sci. Appl. (ICISA)*, 2018, pp. 251–258. [Online]. Available: https://link.springer.com/chapter/10.1007%2F978-981-13-1056-0_26

[16] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Security*, Alexandria, VA, USA, 2006, pp. 89–98.

[17] F. Han, J. Qin, H. Zhao, and J. Hu, "A general transformation from KP-ABE to searchable encryption," *Future Gener. Comput. Syst.*, vol. 30, pp. 107–115, Jan. 2014.

[18] J. Herranz, "Attribute-based versions of Schnorr and ElGamal," *Applicable Algebra Eng. Commun. Comput.*, vol. 27, no. 1, pp. 17–57, 2016.

[19] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *Proc. 17th Int. Conf. Pract. Theory Public Key Cryptography Public Key Cryptography (PKC)*, 2014, pp. 293–310.

[20] C. Jennings, B. Lowekamp, E. Rescorla, S. Baset, and H. Schulzrinne, "Resource location and discovery (RELOAD) base protocol," Internet Eng. Task Force, Fremont, CA, USA, RFC 6940, 2014.

[21] K. Kim and D. Park, "Heterogeneity aware P2P algorithm by using mobile nodeID," in *Proc. Int. Conf. Inf. Netw. Adv. Data Commun. Wireless Netw. (ICOIN)*, Sendai, Japan, 2006, pp. 975–984.

[22] S. Kalra and S. K. Sood, "Secure authentication scheme for IoT and cloud servers," *Pervasive Mobile Comput.*, vol. 23, pp. 210–223, Dec. 2015.

[23] N. Koblitz and A. J. Menezes, "The random oracle model: A twenty-year retrospective," *Designs Codes Cryptography*, vol. 77, nos. 2–3, pp. 587–610, 2015.

[24] O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging security mechanisms for medical cyber physical systems," *IEEE/ACM Trans. Comput. Biol. Bioinformat.*, vol. 13, no. 3, pp. 401–416, May/Jun. 2016.

[25] Y. Liao *et al.*, "Insecurity of a key-policy attribute based encryption scheme with equality test," *IEEE Access*, vol. 6, pp. 10189–10196, 2018.

[26] S. Lin, R. Zhang, H. Ma, and M. Wang, "Revisiting attribute-based encryption with verifiable outsourced decryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 10, pp. 2119–2130, Oct. 2015.

[27] W. Liu, J. Liu, Q. Wu, and B. Qin, "Android PBC: A pairing based cryptography toolkit for android platform," in *Proc. Commun. Security Conf. (CSC)*, Beijing, China, 2014, pp. 1–6.

[28] L. Nkenyereye, Y. Park, and K. H. Rhee, "A secure billing protocol over attribute-based encryption in vehicular cloud computing," *EURASIP J. Wireless Commun. Netw.*, vol. 196, pp. 1–12, Dec. 2016.

[29] D. J. Rani and S. E. Roslin, "Light weight cryptographic algorithms for medical Internet of Things (IoT)—A review," in *Proc. Online Int. Conf. Green Eng. Technol. (IC-GET)*, Coimbatore, India, 2016, pp. 1–6.

[30] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. 24th Annu. Int. Conf. Theory Appl. Cryptograph. Techn. Adv. Cryptol. (EUROCRYPT)*, Aarhus, Denmark, 2005, pp. 457–473.

[31] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[32] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Adv. Cryptol. (CRYPTO)*, Santa Barbara, CA, USA, 1985, pp. 47–53.

[33] S. Singh, P. K. Sharma, S. Y. Moon, and J. H. Park, "Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions," *J. Ambient Intell. Humanized Comput.*, May 2017, pp. 1–18. [Online]. Available: https://link.springer.com/article/10.1007%2Fs12652-017-0494-4

[34] S.-Y. Tan and W.-S. Yap, "Cryptanalysis of a CP-ABE scheme with policy in normal forms," *Inf. Process. Lett.*, vol. 116, no. 7, pp. 492–495, 2016.

[35] S.-Y. Tan, C.-S. Wong, and H.-H. Ng, "An optimized pairing-based cryptography library for Android," *Int. J. Cryptol. Res.*, vol. 6, no. 1, pp. 16–30, 2016.

[36] D. S. Touceda, J. M. S. Cámara, and M. Soriano, "Decentralized certification scheme for secure admission in on-the-fly peer-to-peer systems," *Inf. Netw. Adv. Data Commun. Wireless Peer-to-Peer Netw. Appl.*, vol. 5, no. 2, pp. 105–124, 2012.

[37] S. Wang, J. Wan, D. Zhang, D. Li, and C. Zhang, "Towards smart factory for industry 4.0: A self-organized multi-agent system with big data based feedback and coordination," *J. Comput. Netw.*, vol. 101, pp. 158–168, Jun. 2016.

[38] T. Wu, F. Wu, J.-M. Redouté, and M. R. Yuce, "An autonomous wireless body area network implementation towards IoT connected healthcare applications," *IEEE Access*, vol. 5, pp. 11413–11422, 2017.

[39] B. Xu *et al.*, "Ubiquitous data accessing method in IoT-based information system for emergency medical services," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1578–1586, May 2014.

[40] D. Yang, J. Yang, and B. Chen, "Leveraging certificate-less public key cryptosystem for node ID assignment in structured P2P systems," *Int. J. Security Appl.*, vol. 9 no. 8, pp. 104–112, 2015.

[41] G. Yang *et al.*, "A health-IoT platform based on the integration of intelligent packaging," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2180–2191, Nov. 2015.

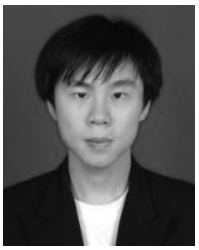
[42] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Future Gener. Comput. Syst.*, vol. 49, pp. 104–112, Aug. 2015.

[43] L. You and L. Wang, "Hierarchical authority key-policy attribute-based encryption," in *Proc. IEEE Int. Conf. Commun. Technol. (ICCT)*, Hangzhou, China, 2015, pp. 868–872.
[44] J. Zarrin, R. L. Aguiar, and J. P. Barraca, "HARD: Hybrid adaptive resource discovery for jungle computing," *J. Netw. Comput. Appl.*, vol. 90, pp. 42–73, Jul. 2017.
[45] L. Zhang, P. Liang, and Y. Mu, "Improving privacy-preserving and security for decentralized key-policy attributed-based encryption," *IEEE Access*, vol. 6, pp. 12736–12745, 2018.
[46] H. Zhu, L. Wang, H. Ahmad, and X. Niu, "Key-policy attribute-based encryption with equality test in cloud computing," *IEEE Access*, vol. 5, pp. 20428–20439, 2017.
[47] S. Zickau, D. Thatmann, A. Butyrtschik, I. Denisow, and A. Kupper, "Applied attribute-based encryption schemes," in *Proc. 19th Int. Conf. Innov. Clouds Internet Netw. (ICIN)*, Paris, France, 2016, pp. 88–95.

Syh-Yuan Tan received the Ph.D. degree in engineering from Universiti Tunku Abdul Rahman, Petaling Jaya, Malaysia in 2015.

He is currently with the School of Computing, Newcastle University, Newcastle upon Tyne, U.K., as a Post-Doctoral Researcher. He was a Senior Lecturer with Multimedia University, Cyberjaya, Malaysia, from 2012 to 2018. His current research interests include cryptography and information security, particularly on provable security techniques.

Dr. Tan served on a committee for Malaysia Cryptographic Standards from 2016 to 2018. He is a member of the Malaysia National Mirror Committee for ISO/IEC on Cryptography and Security Mechanisms, as well as a member of the Malaysian Society for Cryptology Research.



Kin-Woon Yeow received the bachelor of engineering degree from Multimedia University, Cyberjaya, Malaysia, in 2013 and the master's degree from the Faculty of Information Science and Technology, Multimedia University, in 2017. He is currently pursuing the postgraduation degree at Leibniz Universität Hannover, Hanover, Germany.

He was a Software Design Engineer with Sony Research and Development EMCS (M) Pte. Ltd., Bandar Baru Bangi, Malaysia, from 2013 to 2015. His current research interests include modeling, simulation, and network security.

Seong Oun Hwang (M'16–SM'18) received the B.S. degree in mathematics from Seoul National University, Seoul, South Korea, in 1993, the M.S. degree in computer and communications engineering from the Pohang University of Science and Technology, Pohang, South Korea, in 1998, and the Ph.D. degree in computer science from the Korea Advanced Institute of Science and Technology, Daejeon, South Korea.

He was a Software Engineer with LG-CNS Systems, Inc., Seoul, from 1994 to 1996. He was a Senior Researcher with the Electronics and Telecommunications Research Institute (ETRI), Gwangju, South Korea, from 1998 to 2007. Since 2008, he has been a Professor with the Department of Software and Communications Engineering, Hongik University, Seoul. His current research interests include cryptography, cyber security, and artificial intelligence.

He is currently an Editor of the *ETRI Journal*.