IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received February 13, 2019, accepted March 8, 2019, date of publication April 1, 2019, date of current version April 26, 2019.
*Digital Object Identifier 10.1109/ACCESS.2019.2906290*

# A New Encrypted Data Switching Protocol: Bridging IBE and ABE Without Loss of Data Confidentiality

**KAI HE[1], YIJUN MAO[2], JIANTING NING[3,4], KAITAI LIANG[5], XINYI HUANG[3], EMMANOUIL PANAOUSIS[5], AND GEORGE LOUKAS[6]**
[1]School of Software Engineering and Cyperspace Science, Dongguan University of Technology, Dongguan 523808, China
[2]School of Mathmatics and Informatics, South China University of Agriculture, Guangzhou 510642, China
[3]School of Mathematics and Computer Science, Fujian Normal University, Fuzhou 350007, China
[4]Department of Computer Science, National University of Singapore, Singapore 119077
[5]Department of Computer Science, University of Surrey, Guildford GU2 7XH, U.K.
[6]Department of Computing and Information Systems, University of Greenwich, London SE10 9LS, U.K.

Corresponding author: Jianting Ning (ningjt@comp.nus.edu.sg)

This work was supported in part by the Ph.D. Research Startup Foundation, Dongguan University of Technology, under Grant GC300502-2, in part by the National Research Foundation, Prime Minister's Office, Singapore, under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd., and in part by the National Natural Science Foundation of China under Grant 61822202.

**ABSTRACT** Encryption technologies have become one of the most prevalent solutions to safeguard data confidentiality in many real-world applications, e.g., cloud-based data storage systems. Encryption outputting a relatively ''static'' format of encrypted data, however, may hinder further data operations. For example, encrypted data may need to be ''transformed'' into other formats for computation or other purposes. To enable encryption to be used in another device equipped with a different encryption mechanism, the concept of encryption switching was first proposed in CRYPTO 2016 for conversion particularly between Paillier and ElGamal encryptions. This paper considers the conversion between conventional identity-based and attribute-based encryptions and further proposes a concrete construction via the technique of proxy re-encryption. The construction is proved to be CPA secure in the standard model under $q$-decisional parallel bilinear Diffie–Hellman exponent assumption. The performance comparisons highlight that our bridging mechanism reduces computation and communication cost on the client side, especially when the data of the client is encrypted and outsourced to a remote cloud. The computational costs with respect to re-encryption (on the server side) and decryption (on the client side) are acceptable in practice.

**INDEX TERMS** Data security, encryption switching, identity-based encryption, attribute-based encryption, CPA security, standard model.

## I. INTRODUCTION

An interesting and useful primitive of public key cryptography, which is called encryption switching protocol (ESP), has been introduced in CRYPTO 2016 by Couteau *et al.* [1]. The basic idea behind ESP is to build a ''bridge'' between an ElGamal-like ciphertext and a Paillier encryption [2] in such a way that the two different encryptions can transfer from one to the other. For instance, given an encryption of Paillier, ESP can be used to convert the ciphertext to ElGamal-like encryption under the same plaintext, and furthermore, it cannot leak the underlying plaintext in encryption conversion phase. The initial motivation of the design of ESP is to bring convenience and scalability in the transformation between homomorphic computations ($+$ and $\times$), so that even a garbled circuit with only $+$ (resp. $\times$) gates is able to take ElGamal-like (resp. Paillier) encryption as input.

Inspired by the seminal notion, this paper explores the concept of ESP into more general context of public key encryption (PKE). As advanced versions of PKE, identity-based encryption (IBE) [3] and attribute-based encryption (ABE) [4] have been introduced in the literature to enhance

The associate editor coordinating the review of this manuscript and approving it for publication was Zheng Yan.

fine-grained data sharing by allowing the data encryptor to encrypt data under the ''fuzzy'' information of the data receiver. Furthermore, ABE also supports one-to-many data sharing mode in the sense that the data owner only needs to generate an encryption intended for a group of users specified by some descriptions, so that the users can leverage respective decryption keys to reveal the underlying plaintext. Both cryptographic primitives can be implemented in many real-world applications, such as Voltage,[1] Secure Zones [5] and Andraben [6].

*Motivation:* Suppose a local tax authority may send an email to contact a tax payer, say Alice, to ask for necessary documents (e.g., bank details and income) to check if Alice has committed fraud in a tax report. If there is a sender address in the email, Alice may encrypt an audit log of personal online bank transactions under the address for the authority. Upon the arrival of the encrypted message, the gateway of the tax authority may recognize it in order to send the encryption to the most appropriate officials. To do so, the gateway has to decrypt the ciphertext and further re-encrypt it under, say the email address of Bob (who is the official at the tax audit department). If Alice cannot see the address of the sender in the email (note this is quite common in practice, known as ''No-Reply'' email), she may encrypt the file under the descriptions of the authority, for example, (''Tax Authority'' AND ''London Area'' AND (''Audit Dept.'' OR ''Others'')), and further upload the encryption to the authority online. The gateway of the tax authority may do nothing but broadcast the encryption within the internal network. To shorten the response time of handling each auditing case, the gateway may reform the ciphertext intended for specified officials by decrypting the message and re-encrypting under the officials' email addresses. However, both of the above approaches leak sensitive personal information to the gateway.

We may also consider a scenario where a communication channel can only support a special type of encrypted message, say IBE, due to the control of communication bandwidth. However, an ABE ciphertext requests to go through the channel to reach another network domain. Without a secure ciphertext convertor, the gateway of the channel has to decrypt the message to fulfil the transformation of encryption. *How to allow one to securely convert the ciphertexts without gaining access to the underlying plaintext that motivates this work.*

The conversion between encryptions with different domains may bring convenience in data analysis and communication. For instance, in the context of big data aggregation, a data collector may receive various formats of data from many sources. It is challenging for the collector to aggregate the data if they are encrypted in different domains. A naive way of data aggregation here is first to request all the data sources to provide decryption keys and further to fulfil expensive decryption. But this method requires sharing of the secret keys, which can lead to potential data security breach to the data sources. *How to allow one to securely share data without sharing secret key is also a motivation of our work.*

[1] https://www.voltage.com/technology/data-encryption/identity-based-encryption/

Under the umbrella of EPS, this paper considers the conversion between IBE and ABE.

*Difficulty:* It is challenging to achieve our goal - designing an encryption switching scheme to bridge IBE and ABE via proxy re-encryption (PRE) technique. In the literature, only Mizuno and Doi [7] have proposed an $ABE \rightarrow IBE$ type PRE construction that is able to convert a ciphertext in the format of ABE to an IBE encryption. The scheme, however, cannot achieve the conversion for the other way round, i.e. converting an IBE ciphertext to an ABE encryption. Besides, reference [7] only supports AND gates on positive and negative attributes w.r.t. ABE encryption, which offers low expressiveness. The construction proposed in this paper will not be limited to the above issues. Yet, the main difficulty depends on how to construct re-encryption key to (i) enable bilateral conversion and (ii) minimize the effect expressiveness (in terms of ABE). In order to construct a re-encryption key we usually need to input the secret/private key of a delegator (i.e. original data owner) and the public key information (or ID, attributes) of a delegatee (i.e. the data receiver after conversion). Here, we give the re-encryption key construction in [7] as an example whereby $g^{\alpha_1}$ and $g^{at}$ are parts of the private key of delegator and meanwhile $ID$ is the public identity of delegatee. However, the part $g^{\alpha_1} g^{at} (g^{ID} h)^w$ is the hindrance to prevent the conversion from IBE to ABE. To bypass this hindrance, in our construction, we design a re-encryption key from the private key of delegator and a partial private key of delegatee. The re-encryption key actually contains the delegator's private key and an IBE ciphertext. When being used to convert an ABE ciphertext to an IBE one, the re-encryption algorithm runs the ABE decryption and further outputs the decryption results which is an IBE ciphertext. In this case, we must guarantee that, given a re-encryption key, proxy cannot obtain any information of the underling plaintext, even if it colludes with the corresponding delegatee (who is without knowledge of the delegator's private key). To achieve the guarantee, we randomize the private keys of both delegator and delegatee. Besides, we require that the hard assumptions of the underlying ABE and IBE should be the same or at least, have an inclusive relationship.

*Identity-Based Encryption:* Identity-based cryptography is a general extension of public-key cryptography where the public key of a user can be any arbitrary string uniquely representing the identity of the user (e.g. name or email address). In 1984, Shamir first proposed the concept of IBE [3]. Till 2001, the first construction of IBE was constructed by Boneh and Franklin [8] by using Weil pairing. However, the security proof is based on the random oracle model. In 2004, Boneh and Boyen presented an IBE scheme with IND-ID-CPA security in the standard model [9], and later Waters [10] proposed a more efficient IBE scheme. Since its introduction, IBE has been explored to support

**TABLE 1. Comparison with Related Works.**

| Scheme | Type | Complexity Assumption | Security | Standard Model |
|---|---|---|---|---|
| [9] | IBE | decisional bilinear Diffie-Hellman (DBDH) | CPA | √ |
| [18] | ABE | decisional $q$-parallel BDHE | CPA | √ |
| [33] | PKE→IBE | DBDH | CPA | √ |
| [7] | ABE→IBE | DBDH | CPA | √ |
| [1] | Paillier↔ElGammal | decisional composite residuosity, decisional Diffie-Hellman, quadratic residuosity assumptions | CPA | √ √ |
| Ours | IBE↔ABE | decisional $q$-parallel BDHE | CPA | √ |

various features, e.g., anonymous IBE [11], [12], hierarchical IBE [13], identity-based broadcast encryption [14] and revocable IBE [15].

*Attribute-Based Encryption:* ABE is an extension of IBE. It allows private key and ciphertext to be labeled with descriptions, so that a decryption is valid if and only if the description of a decryption key matches that of a ciphertext. It has been widely employed in fine-grained data access control. There are two important variants of ABE, one is key-policy ABE (KP-ABE) [4] relating access control policy to decryption key, and the other is ciphertext-policy ABE (CP-ABE) [16], [17] associating ciphertext with access control policy. Since its introduction, ABE has been extended to support various features, e.g., large universe ABE [18], [19], traceable ABE [20], [21] and outsourced ABE [22], [23].

*Proxy re-encryption:* Blaze *et al.* [24] introduced the notion of PRE in the context of PKE. In a PRE system, a delegator, say Alice, can request a semi-trusted proxy to transform a ciphertext under her public key to another ciphertext under the public key of a delegatee, say Bob, without leaking the underlying information of the plaintext to the proxy. Some variants of traditional PRE have been proposed in the literature (e.g. [25]–[27]). In 2007, Green and Ateniese [28] explored PRE in the context of IBE and further introduced the notion of the identity-based PRE (IBPRE). To implement PRE in the attribute-based cryptographic setting, Liang *et al.* [29] defined CP-ABPRE, and proposed a concrete construction on top of [30]. Following the seminal work, ABPRE have been proposed to achieve better security and more expressiveness in data sharing [31].

However, all the aforementioned schemes cannot support encryption switching. A hybrid proxy PRE was first proposed by Matsuo [32] in 2007 to enable a PKE ciphertext to be converted to an IBE one. Later, Mizuno and Doi [7] proposed a PRE conversion from ABE to IBE while maintaining the confidentiality of plaintext. Recently, Couteau *et al.* [1] introduced an encryption switching between Paillier and ElGamal based on homomorphic encryption. We compare our construction with [1], [7], [9], [17], and [32] in terms of functionality, security and feature in Table 1. The details of efficiency analysis will be given in Section 5. We state that our scheme is the first of its type to achieve bidirectional conversion between ABE and IBE with CPA security in the standard model.

### A. ORGANIZATION

The rest of this paper is organized as follows. In Section 2, we briefly review the complexity assumption, definitions and security notion used in this paper. In Section 3 we present the construction. In Section 4, we give the security proof. In Section 5, we compare our work with other related works in terms of efficiency. In Section 6, we present the conclusion.

## II. PRELIMINARIES

### A. BILINEAR GROUPS AND COMPLEXITY ASSUMPTION

Two multiplicative cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ whose orders are prime $p$ and a bilinear map $e : \mathbb{G}\times\mathbb{G} \to \mathbb{G}_T$ has the following three properties:

- **Bilinearity:** $e(g^a, h^b) = e(g, h)^{ab}$ for all $g, h \in \mathbb{G}$ and $a, b \in \mathbb{Z}_p$.
- **Non-degeneracy:** There exist $g, h \in \mathbb{G}$ such that $e(g, h) \neq 1_{\mathbb{G}}$.
- **Computability:** There exists an efficient algorithm to compute $e(g, h)$ for all $g, h \in \mathbb{G}$.

**Decisional Parallel Bilinear Diffie-Hellman Exponent Assumption [17].** Given a group $\mathbb{G}$ of prime order $p$, let $a, s, b_1, \cdots, b_q \in_R \mathbb{Z}_p$ and $g$ be a generator of $\mathbb{G}$. If an algorithm is given $\overrightarrow{y} = g, g^s, g^a, \cdots, g^{a^q}, , g^{a^{q+2}}, \cdots, g^{a^{2q}}$

$$\forall 1 \leq j \leq q \quad g^{s\cdot b_j}, g^{a/b_j}, \cdots, g^{a^q/b_j}, , g^{a^{q+2}/b_j}, \cdots, g^{a^{2q}/b_j}$$

$$\forall 1 \leq j, k \leq q, k \neq j \quad g^{a\cdot s\cdot b_k/b_j}, \cdots, g^{a^q\cdot s\cdot b_k/b_j}$$

It is hard to distinguish $e(g, g)^{a^{q+1}s} \in \mathbb{G}_T$ from a random element in $\mathbb{G}_T$.

The advantage $\varepsilon$ of an adversary $\mathcal{A}$ to solve decisional q-parallel BDHE if

$$|Pr[\mathcal{A}(\overrightarrow{y}, T = e(g, g)^{a^{q+1}s}) = 0] - Pr[\mathcal{A}(\overrightarrow{y}, T = R) = 0]| \geq \varepsilon$$

### B. DEFINITION OF ATTRIBUTE-BASED ENCRYPTION

*Definition 1:* An attribute-based encryption (ABE) usually consists of four algorithms.

**ABE.Setup**($\lambda$, $U$): intake a security parameter $\lambda$ and description universe, output the public parameters $PK$ and a master key $MSK$. We assume that $PK$ is implicitly seen as input for the following algorithms.

**ABE.KeyGen**($MSK$, $\mathbb{A}$): intake the master key $MSK$ and a description $\mathbb{A}$, output a private key $SK$.

**ABE.Encrypt**($\mathcal{M}$, $\mathbb{B}$): intake a message $\mathcal{M}$, and a description $\mathbb{B}$, output a ciphertext $CT$.

**ABE.Decrypt**$(CT, SK)$: intake a ciphertext $CT$ which contains a description $\mathbb{A}$, and a private key $SK$ corresponding to another description $\mathbb{B}$. If $\mathbb{B}$ matches $\mathbb{A}$ the algorithm decrypts the ciphertext and returns a message $\mathcal{M}$; otherwise, return $\perp$.

While $\mathbb{A}$ is a set of attributes over $U$ and $\mathbb{B}$ is an access policy, the definition is for KP-ABE; if the case is the other way round, that is for CP-ABE.

### C. DEFINITION OF IDENTITY-BASED ENCRYPTION

*Definition 2:* Following Definition 1, if we set $\mathbb{A} = \mathbb{B}$ as an identity of a system user, we have the definition for IBE.

### D. DEFINITION OF ENCRYPTION SWITCHING

We here define a general ciphertext conversion framework between ABE and IBE.

*Definition 3:* Following Definition 1 and 2, we have the definition of encryption switching (ES):

**ES.Setup**$(\lambda, U)$: $(ABE.PK, ABE.MSK) \leftarrow$ ABE.Setup$(\lambda, U)$ and $(IBE.PK, IBE.MSK) \leftarrow$ IBE.Setup$(\lambda, U)$. Set $PK = (ABE.PK, IBE.PK)$ and $MSK = (ABE.MSK, IBE.MSK)$. We note that $\lambda$ is the same security parameter and the $ABE.PK, IBE.PK$ could be held by two distinct trusted parties, respectively.

**ES.KeyGen**$(MSK, \mathbb{A})$: $SK_{\mathbb{A}} \leftarrow \delta.KeyGen(MSK, \mathbb{A})$, where $\delta \in \{ABE, IBE\}$ and $\mathbb{A} \in \{an\ attribute\ set, anaccess\ policy, an\ identity\}$.

**ES.ReKeyGen**$(\mathbb{A}, \mathbb{B}, SK_{\mathbb{A}}, SK_{\mathbb{B}})$: intake the descriptions $\mathbb{A}$, $\mathbb{B}$ and private keys $SK_{\mathbb{A}}$, $SK_{\mathbb{B}}$, output a re-encryption key $RK_{\mathbb{A}\to\mathbb{B}}$, where $\mathbb{A}$ and $\mathbb{B}$ are from distinct encryption mechanisms, e.g., $\mathbb{A} \in \{an\ attribute\ set, \ an\ access\ policy\}$ and $\mathbb{B}$ is an identity.

**ES.Encrypt**$(\mathcal{M}, \mathbb{A})$: $CT_{\mathbb{A}} \leftarrow \delta.Encryption(\mathcal{M}, \mathbb{A})$. We assume that ABE and IBE share the same message domain in the definition.

**ES.ReEncrypt**$(CT_{\mathbb{A}}, RK_{\mathbb{A}\to\mathbb{B}})$: intake a ciphertext $CT_{\mathbb{A}}$ under the description $\mathbb{A}$ and a re-encryption key $RK_{\mathbb{A}\to\mathbb{B}}$, output a re-encrypted ciphertext $CT_{\mathbb{B}}$.

**ES.Decrypt**$(CT, SK)$: $\mathcal{M}/\perp \leftarrow \delta.Decrypt(CT, SK)$.

Note that we assume the above conversion definition between ABE and IBE should share the same message domain $\mathcal{M}$ (so that the conversion can be executed smoothly).

### E. SECURITY MODEL OF ENCRYPTION SWITCHING ABE↔IBE IN GAME-BASED FRAMEWORK

The selectively chosen plaintext security against ABE→IBE type ES is defined as the following game between an attacker $\mathcal{A}$ and a challenger $\mathcal{C}$. The game describes the security of the underlying ABE and IBE scheme even if $\mathcal{A}$ achieves re-encryption keys which can transform the ciphertext of ABE to the one of IBE.

**Init.** $\mathcal{A}$ chooses a target access structure $\mathbb{A}^*$ and a target IBE identity $ID^*$, and sends them to $\mathcal{C}$.

**Setup.** $\mathcal{C}$ runs $Setup_A(1^\kappa)$ and $Setup_I(1^\kappa)$, and returns ABE public parameters and IBE public parameters to the $\mathcal{A}$.

**Phase 1.** $\mathcal{A}$ is allowed to adaptively issue ABE private key queries, IBE private key queries and re-encryption key queries as follows:

- $Extract_A(S)$ : $\mathcal{A}$ can adaptively and repeatedly request an ABE private key for a set $S$ where $S \not\models \mathbb{A}^*$.
- $Extract_I(ID, params)$: $\mathcal{A}$ can adaptively and repeatedly issue an IBE private key corresponding to an identity $ID$ of his choice.
- $Extract_{A\to I}(S, ID)$: $\mathcal{A}$ can adaptively and repeatedly request re-encryption key which can transform ABE ciphertexts encrypted for set $S$ to IBE ciphertexts corresponding to an identity $ID$. (It is only with the security of [ABE-IBE] type proxy re-encryption scheme)

**Challenge.** $\mathcal{A}$ submits two equal length messages $M_0$ and $M_1$ and selects which scheme to attack (ABE or IBE). $\mathcal{C}$ randomly chooses $\beta \in \{0, 1\}$ and returns the encrypted result of $M_\beta$ encrypted by the selected scheme.

**Phase 2.** Same as Phase 1.

**Guess.** $\mathcal{A}$ submits a guess $\beta' \in \{0, 1\}$. If $\beta' = \beta$, $\mathcal{A}$ wins.

During Phase 1 and 2, $\mathcal{A}$ is restricted to the following queries:

- $Extract_A(S)$, where $S \models \mathbb{A}^*$.
- $Extract_I(ID^*)$.
- $Extract_{A\to I}(S^*, ID)$ and $Extract_I(ID, param)$ queries, where $S \models \mathbb{A}^*$ and $ID$ is an arbitrary IBE user's identity.

*Remark:* The selectively chosen plaintext security against IBE→ABE type ES is similar to the above security game except the queries of re-encryption key $Extract_{I\to A}(ID, S)$ where the re-encryption key transforms IBE under an identity $ID$ to ABE under a description $S$.

*Definition 4:* We define $\mathcal{A}$'s advantage in the above game as $Adv_A(1^\kappa) = 2Pr[\beta' = \beta] - 1$. We state that an ABE→IBE (resp. IBE→ABE) type ES is indistinguishable under selectively chosen plaintext attacks, if for any probabilistic polynomial time (PPT) adversary $\mathcal{A}$, the advantage in the security game is negligible.

## III. CONSTRUCTIONS

### A. BUILDING BLOCKS REVIEW

Our ES between ABE and IBE is built on top of Waters-ABE scheme [17] and the first construction of BB-IBE [9]. We are going to review them as follows.

**Waters-ABE Construction.** Waters-ABE consists of the following four algorithms [17].

**Setup**$(\lambda, U)$. Let $U$ be the maximum number of system attributes. Let $\mathbb{G}, \mathbb{G}_T$ be a bilinear group of prime order $p$. Let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. Then, it chooses a generator $g$ as well as random group elements $h_1, \cdots, h_U \in \mathbb{G}$ that are associated with the $U$ attributes in the system. In addition, it chooses random exponents $\alpha_1, a \in \mathbb{Z}_p$. The public key is

$$PK_1 = g, e(g, g)^{\alpha_1}, g^a, h_1, \cdots, h_U.$$

The master private key is $MSK_1 = g^{\alpha_1}$.

**Encrypt**$(PK_1, \mathcal{M}, (M, \rho))$. It takes as input the public parameters $PK_1$, a message $\mathcal{M}$ as well as an LSSS access structure $(M, \rho)$, where $M$ be an $\ell \times n$ matrix and $\rho$ associates rows of $M$ to attributes. It first chooses a vector

$\vec{v} = (s, y_2, \cdots, y_n) \in_R \mathbb{Z}_p^n$. These values will be used to share the encryption exponent $s$. For $i = 1$ to $\ell$, it calculates $\lambda_i = \vec{v} \cdot M_i$, where $M_i$ is the vector corresponding to the $i$th row of $M$. Then it chooses $r_1, \cdots, r_\ell \in_R \mathbb{Z}_p$ and computes the ciphertext as follows:

$$C = \mathcal{M} \cdot e(g, g)^{\alpha_1 s},$$
$$C' = g^s, \quad \{C_i = g^{a\lambda_i} h_{\rho(i)}^{-r_i}, \; D_i = g^{r_i}\}_{i \in \{1, \cdots, \ell\}}$$

The ciphertext is $CT_S = (C, C', \{C_i, D_i\}_{\rho(i) \in M})$ along with a description of $(M, \rho)$.

**KeyGen**$(MSK_1, S)$. It takes as input the master private key $MSK_1$ and a set $S$ of attributes. It chooses $t \in_R \mathbb{Z}_p$ and creates the private key $SK_S = (K, L, \{K_x\}_{x \in S})$ as

$$K = g^{\alpha_1} g^{at}, \quad L = g^t, \; \forall x \in S: \; K_x = h_x^t$$

**Decrypt**$(CT, SK_S)$. It takes as input a ciphertext $CT$ for a linear access structure $(M, \rho)$ and a private key $SK_S$. Suppose that $S$ satisfies the access structure and let $I \subset \{1, 2, \cdots, \ell\}$ be defined as $I = \{i : \rho(i) \in S\}$. Then, let $\{w_i \in \mathbb{Z}_p\}_{i \in I}$ be a set of constants such that if $\{\lambda_i\}$ are valid shares of any secret $s$ according to $M$, then $\sum_{i \in I} w_i \lambda_i = s$. It computes

$$\mathcal{M} = \frac{C \cdot \prod_{i \in I} \left(e(C_i, L) e(D_i, K_{\rho(i)})\right)^{w_i}}{e(C', K)} = \frac{\mathcal{M} \cdot e(g, g)^{\alpha_1 s} \cdot \prod_{i \in I} e(g, g)^{a\lambda_i w_i t}}{e(g, g)^{\alpha_1 s} e(g, g)^{ast}}$$

**BB-IBE.** We review BB-IBE [9] construction as follows.

**Setup**$(\lambda)$. Let $\mathbb{G}, \mathbb{G}_T$ be a bilinear group of prime order $p$, and $e : \mathbb{G} \times \mathbb{G} \to G_T$ be the bilinear map. Given a security parameter $\lambda$ as input, the algorithm selects a generator $g_0 \in_R \mathbb{G}$ and $h, g_2 \in_R \mathbb{G}$. It picks $\alpha_2 \in_R \mathbb{Z}_p$ and sets $g_1 = g_0^{\alpha_2}$. The public parameters are $PK_2 = (g_0, g_1, g_2, h)$ and the master private key is $MSK_2 = \alpha_2$.

**Encrypt**$(ID, PK_2, \mathcal{M})$. Given an identity $ID$, public parameter $PK_2$ and plaintext $\mathcal{M} \in \mathbb{G}_T$ as input, the algorithm selects $w \in_R \mathbb{Z}_p$ and outputs an IBE ciphertext $CT_{ID}$.

$$CT_{ID} = (C_1, C_2, C_3) = (g_0^w, (g_1^{ID} h)^w, \mathcal{M} e(g_1, g_2)^w)$$

**KeyGen**$(MSK_2, PK_2, ID)$. Given master private key $MSK_2$, public parameters $PK_2$ and an identity $ID$ as input, the algorithm picks $u \in_R \mathbb{Z}_p$ and outputs an IBE private key as

$$SK_{ID} = (SK_{ID}^1, SK_{ID}^2) = (g_2^{\alpha_2} (g_1^{ID} h)^u, g_0^u).$$

**Decrypt**$(SK_{ID}, CT_{ID})$. Given an IBE private key $SK_{ID}$ and an IBE ciphertext $CT_{ID}$ as input, the algorithm outputs a plaintext $\mathcal{M}$.

$$\mathcal{M} = \frac{C_3 \cdot e(SK_{ID}^2, C_2)}{e(SK_{ID}^1, C_1)}$$

### *B. CONSTRUCTION: ABE→IBE TYPE ES*

Based on the above ABE and IBE schemes, we design an ES via PRE technique which converts the encryption of ABE to that of IBE scheme. We define that $ES.Setup$ =[Setup$(\lambda, U)$, Setup$(\lambda)$], $ES.KeyGen$ = [KeyGen$(MSK_1, S)$, KeyGen$(MSK_2, PK_2, ID)$], and $ES.Encrypt$ = [Encrypt$(PK_1, \mathcal{M}, (M, \rho))$, Encrypt$(ID, PK_2, \mathcal{M})$]. The main technique we introduce here is to build a plug-in to convert two types of encryption, so that we only focus on the algorithms related to the conversion, namely ES.ReKenGen, ES.ReEncrypt and ES.Decrypt. For the setup, key generation and encryption, one may use the respective algorithm depending on which encryption domain he/she is currently in, for example, one may use the algorithm Encrypt$(ID, PK_2, \mathcal{M})$ to encrypt data if he/she is in the context of IBE.

**ES.ReKenGen**$_{A\to I}(PK_1, PK_2, S, ID, SK_S, SK_{ID}^2)$: Given the ABE and IBE public parameter $PK_1$ and $PK_2$, attribute set $S$ and a delegator $B$'s ABE private key $SK_S$, a delegatee $A$'s IBE identity $ID$ and its 2nd component of private key $SK_{ID}^2$ as input, the algorithm outputs a re-encryption key $RK_{A\to I} = (R_a, R_b, R_c, R_d, rk_1, \{rk_x\}_{x \in S})$ as follows:

- Client $A$ chooses $u' \in_R \mathbb{Z}_p$ and computes $SK_{ID}^{2\,\prime} = SK_{ID}^2 \cdot g_0^{u'} = g_0^{u''}$, where $u + u' = u''$. Then client $A$ returns $SK_{ID}^{2\,\prime}$ to client $B$ and keeps secret $u'$ which is needed in the decryption algorithm.
- Client $B$ selects $t' \in_R \mathbb{Z}_p$ and sets
$$R_a = K \cdot g^{at'} \cdot SK_{ID}^{2\,\prime} = g^{\alpha_1} g^{at''} g_0^{u''}.$$
Client $B$ selects $\tau \in_R \mathbb{Z}_p$ and sets
$$R_b = g_0^\tau, \quad R_c = (g_1^{ID} h)^\tau, \; R_d = e(g_1, g_2)^\tau.$$
Client $B$ computes $rk_1 = L \cdot g^{t'} = g^{t''}$.
For each attribute $x \in S$: $rk_x = K_x \cdot h_x^{t'} = h_x^{t''}$, where $t + t' = t''$.

**ES.ReEncrypt**$_{A\to I}(RK_{A\to I}, CT_S)$: Given attribute set $S$, identity $ID$, a re-encryption key $RK_{A\to I}$ and an ABE ciphertext $CT_S = (C, C', \{C_i, D_i\}_{\rho(i) \in M})$ along with a description of $(M,\rho)$ as input, output an IBE ciphertext $CT_{ID} = (\overline{C_1}, \overline{C_2}, \overline{C_3})$ as follows:

Suppose $S$ satisfies the access structure $(M, \rho)$ and let $I \subset \{1, 2, \cdots, \ell\}$ be defined as $I = \{i : \rho(i) \in S\}$. Then, let $\{w_i \in \mathbb{Z}_p\}_{i \in I}$ be a set of constants such that if $\{\lambda_i\}$ are valid shares of any secret s according to $M$, then $\sum_{i \in I} w_i \lambda_i = s$. Compute $C_i' = e(C_i, rk_1) e(rk_i, D_i) = e(g, g)^{a\lambda_i t''}$.

Select $y \in_R \mathbb{Z}_p$ and compute:

$$\overline{C_1} = R_b^y = g_0^{\tau y}$$
$$\overline{C_2} = R_c^y \cdot C' = (g_1^{ID} h)^{\tau y} \cdot g^s$$
$$\overline{C_3} = \frac{C \cdot R_d^y \cdot \prod_{i \in I} C_i'^{w_i}}{e(C', R_a)} = \mathcal{M} \cdot \frac{e(g_1, g_2)^{\tau y}}{e(g^s, g_0^{u''})}$$

**ES.Decrypt**$(PK_2, CT_{ID}, SK_{ID})$: Given IBE public parameters $PK_2$, ciphertext $CT_{ID}$ and private key $SK_{ID}$ of identity $ID$, client $A$ uses $u'$ and computes

$$\mathcal{M} = \frac{\overline{C_3} \cdot e(SK_{ID}^2 \cdot g_0^{u'}, \overline{C_2})}{e\left(SK_{ID}^1 \cdot (g_1^{ID} h)^{u'}, \overline{C_1}\right)} = \frac{\mathcal{M} \cdot e(g_1, g_2)^{\tau y} e(g_0^{u''}, (g_1^{ID} h)^{\tau y} \cdot g^s)}{e(g^s, g_0^{u''}) e\left(g_2^{\alpha} (g_1^{ID} h)^u (g_1^{ID} h)^{u'}, g_0^{\tau y}\right)}$$

### C. IBE→ABE TYPE ES

We further design IBE→ABE Type ES which converts ciphertexts of IBE to ABE format as follows. Similarly, we focus on the algorithms supporting ciphertext conversion.

**ES.ReKenGen**$_{I\to A}(PK_1, PK_2, S, ID, SK_{ID}, SK_S)$: Given ABE and IBE public parameter $PK_1$ and $PK_2$, attribute set $S$ and a delegator $B$'s ABE private key $SK_S$, a delegatee's IBE identity $ID$ and an IBE user $A$'s private key $SK_{ID}$ as input, output a re-encryption key $RK_{I\to A} = (R_a, R_b, \{R_{ci}\}_{\rho(i)\in M'}, R_d, rk_1, rk_2)$ as follows:

- Client $B$ chooses $t' \in_R \mathbb{Z}_p$ and computes $K' = K\cdot g^{at'} = g^{\alpha_1}g^{at''}$, where $t + t' = t''$. Client $B$ sends $K'$ to client $A$ and keeps secret $t'$ which is needed in the decryption algorithm.
- Client $A$ selects $u' \in_R \mathbb{Z}_p$ and sets

$$R_a = SK_{ID}^1 \cdot (g_1^{ID}h)^{u'} \cdot K' = g_2^{\alpha_2}(g_1^{ID}h)^{u''}g^{\alpha_1}g^{at''}$$

Client $A$ selects $\tau \in_R \mathbb{Z}_p$ and sets $R_b = g^{\tau}$.
Let $M'$ be an $\ell \times n$ matrix. The algorithm chooses a random vector $\vec{v'} = (\tau, y_2', \cdots, y_n') \in \mathbb{Z}_p^n$, which will be used to share the encryption exponent $\tau$.
For $i = 1$ to $\ell$, it calculates $\lambda_i' = \vec{v'}\cdot M_i'$, where $M_i'$ is the vector corresponding to the $i$th row of $M'$. In addition, it chooses random $r_i' \in \mathbb{Z}_p$ and computes

$$R_{ci} = \{C_i = g^{a\lambda_i'}h_{\rho(i)}^{-r_i'}, \quad D_i = g^{r_i'}\}, \quad R_d = e(g,g)^{\alpha_1\tau}$$

Client $A$ chooses $\delta \in \mathbb{Z}_p$ and computes

$$rk_1 = sk_{ID}^2 \cdot g_0^{u'} \cdot g_0^{\delta} = g_0^{u''+\delta}, \quad rk_2 = (g_1^{ID}h)^{\delta}$$

**ES.ReEncrypt**$_{I\to A}(RK_{I\to A}, CT_{ID})$: Given a re-encryption key $RK_{I\to A} = (R_a,, R_b, \{R_{ci}\}_{\rho(i)\in M'}, R_d, rk_1, rk_2\})$ and an IBE ciphertext $CT_{ID} = (C_1, C_2, C_3)$ as input, output an ABE ciphertext $CT_S = (\{\overline{C_{1i}}\}_{\rho(i)\in M'}, \overline{C_2}, \overline{C_3}, \overline{C_4})$ as follows:

$$\overline{C} = \frac{e(C_2, rk_1)}{e(C_1, rk_2)} = \frac{e\left((g_1^{ID}h)^w, g_0^{u''+\delta}\right)}{e\left(g_0^w, (g_1^{ID}h)^{\delta}\right)} = e\left((g_1^{ID}h)^w, g_0^{u''}\right)$$

Chooses $y \in \mathbb{Z}_p$, for $\rho(i) \in M_i'$, compute

$$\begin{aligned}\overline{C_{1i}} &= R_{ci}^y \\ &= \{\overline{C_i} = C_i^y = (g^{a\lambda_i'}h_{\rho(i)}^{-r_i'})^y, \overline{D_i} = D_i^y = (g^{r_i'})^y\} \\ \overline{C_2} &= R_b^y \cdot C_1 = g^{\tau y}\cdot g_0^w \\ \overline{C_3} &= R_d^y = e(g,g)^{\alpha_1\tau y}\end{aligned}$$

$$\overline{C_4} = \frac{C_3\cdot\overline{C}}{e(R_a, C_1)} = \frac{\mathcal{M}\cdot e(g_1,g_2)^w \cdot e\left((g_1^{ID}h)^w, g_0^{u''}\right)}{e\left(g_2^{\alpha_2}(g_1^{ID}h)^{u''}\cdot g^{\alpha_1}g^{at''}, g_0^w\right)} = \frac{\mathcal{M}}{e(g^{\alpha_1}g^{at''}, g_0^w)}$$

**ES.Decrypt**$(CT_S, SK_S)$: Given ciphertext $CT_S$ and private key $SK_S$, let $I \subset \{1, 2, \cdots, \ell\}$ be defined as $I = \{i : \rho(i) \in S\}$. Then, let $\{w_i \in \mathbb{Z}_p\}_{i\in I}$ be a set of constants such that if $\{\lambda_i'\}$ are valid shares of any secret $\tau$ according to $M$, then $\sum_{i\in I} w_i\lambda_i' = \tau$.

The decryption algorithm uses $t'$ and computes

$$\mathcal{M} = \frac{\overline{C_4}\cdot e\left(\overline{C_2}, K\cdot g^{at'}\right)}{\prod_{i\in I}\left(e(\overline{C_i}, L\cdot g^{t'})\cdot e(\overline{D_i}, K_{\rho(i)}\cdot h_{\rho(i)}^{t'})\right)^{w_i}\cdot\overline{C_3}} = \frac{\mathcal{M}\cdot e\left(g^{\tau y}g_0^w, g^{\alpha_1}g^{at''}\right)}{e(g^{\alpha_1}g^{at''}, g_0^w)\cdot\left(\prod_{i\in I} e(g,g)^{t''ay\lambda_i'w_i}\right)\cdot e(g,g)^{\alpha_1\tau y}}$$

## IV. SECURITY ANALYSIS

We first prove that our ABE→IBE type ES is indistinguishable under selectively chosen plaintext attacks (IND-sCPA), if the decisional q-parallel BDHE assumption holds.

*Theorem 1:* Suppose the decisional q-parallel BDHE assumption holds, our ABE→IBE type ES is IND-sCPA secure with a challenge matrix of size $\ell^* \times n^*$, where $\ell^*, n^* \le q$.

*Proof:* Suppose we have an adversary $\mathcal{A}$ with non-negligible advantage against the ABE→IBE type ES. We construct an algorithm $\mathcal{B}$ which can solve the decisional q-parallel BDHE problem by using $\mathcal{A}$.

**Init.** $\mathcal{A}$ chooses a target access structure $\mathbb{A}^*$ and a target identity $ID^*$, and sends them to $\mathcal{B}$.

**Setup.** $\mathcal{B}$ Setup simulation as follows:

ABE Setup. $\mathcal{B}$ chooses $\alpha' \in_R \mathbb{Z}_p$ and implicitly sets $\alpha = \alpha' + a^{q+1}$ by letting

$$e(g,g)^{\alpha_1} = e(g^a, g^{a^q})e(g,g)^{\alpha'}.$$

For each attribute $x \in U$, $\mathcal{B}$ chooses a values $z_x \in_R \mathbb{Z}_p$. Let $X$ denote the set of indices $i$, such that $\rho^*(i) = x$, $\mathcal{B}$ sets

$$h_x = g^{z_x}\prod_{i\in X} g^{aM_{i,1}^*/b_i}\cdot g^{a^2M_{i,2}^*/b_i}\cdots g^{a^{n^*}M_{i,n^*}^*/b_i}.$$

Note that if $X = \Phi$ then sets $h_x = g^{z_x}$. $\mathcal{B}$ sends the public parameters $g, e(g,g)^{\alpha_1}, g^a, \{h_x\}_{\rho^*(i)\in U}$ to $\mathcal{A}$.

IBE-Setup. $\mathcal{B}$ chooses $z_1, z_2, z_3 \in_R \mathbb{Z}_p^*$ and sets $g_0 = g, g_1 = g^{az_1}, g_2 = g^{a^q z_2}, h = g_1^{-ID^*}g^{z_3}$. $\mathcal{B}$ sets the master private key $MSK = az_1$. $\mathcal{B}$ sends the public parameters $g_0, g_1, g_2, h$ to $\mathcal{A}$.

**Phase 1.** $\mathcal{A}$ adaptively interacts with $\mathcal{B}$ as follows:

- *Extract*$_A(S)$. $\mathcal{A}$ queries the ABE private key $SK_S$ with a set $S$, where $S \not\models \mathbb{A}^*$.
$\mathcal{B}$ first finds a vector $\vec{w} = (w_1, \cdots, w_{n^*}) \in \mathbb{Z}_p$ such that $w_1 = -1$ and for all $i$ where $\rho^*(i) \in S$ we have that $\vec{w}\cdot M_i^* = 0$. Then $\mathcal{B}$ chooses $r \in_R \mathbb{Z}_p$.
$\mathcal{B}$ defines $t = r + w_1a^q + w_2a^{q-1} + \cdots + w_{n^*}a^{q-n^*+1}$.
It lets

$$L = g^r\prod_{i=1,\cdots,n^*}\left(g^{a^{q+1-i}}\right)^{w_i} = g^t.$$

$\mathcal{B}$ computes $K = g^{\alpha'} g^{ar} \prod_{i=2,\cdots,n^*} \left(g^{a^{q+2-i}}\right)^{w_i}$. For $x \in S$ and there is no $i$ such that $\rho^*(i) = x$, $\mathcal{B}$ defines $K_x = L^{z_x}$.
For $x \in S$ and let $X$ be the set of all $i$ such that $\rho^*(i) = x$, $\mathcal{B}$ defines

$$K_x = L^{z_x} \prod_{i \in X} \prod_{j=(1,n^*)} \left( g^{\frac{a^j \cdot r}{b_i}} \prod_{\substack{k=(1,n^*) \\ k \neq j}} \left(g^{a^{q+1+j-k/b_i}}\right)^{w_k} \right)^{M^*_{i,j}}$$

$\mathcal{B}$ returns $SK_S$ to $\mathcal{A}$ and records the tuple $(S, SK_S)$ in an ABE private key List (ASKL).

- $Extract_I(ID)$. $\mathcal{A}$ queries the IBE user's private key $SK_{ID}$ with an identity $ID$.
  - If $ID = ID^*$, $\mathcal{B}$ rejects.
  - If $ID \neq ID^*$, $\mathcal{B}$ checks the list of $REKL$, and if there exits the re-encryption key to $ID$ and $S \models W$, $\mathcal{B}$ rejects. Otherwise, $\mathcal{B}$ chooses $u \in_R \mathbb{Z}_p$ and computes

$$SK^1_{ID} = g^{\frac{-a^q z_2 z_3}{(ID-ID^*)}} \left(g^{a z_1 (ID-ID^*)} g^{z_3}\right)^u,$$
$$SK^2_{ID} = g^{\frac{-a^q z_2}{(ID-ID^*)}} g^u$$

  $\mathcal{B}$ returns $SK_{ID} = (SK^1_{ID}, SK^2_{ID})$ to $\mathcal{A}$ and records the tuple $(ID, SK_{ID})$ in an IBE private key list (ISKL).

- $Extract_{A \to I}(S, ID)$. $\mathcal{A}$ queries the re-encryption key from attribute set $S$ to identity $ID$ as follows:
  If $S \not\models M^*$: $\mathcal{B}$ runs $Extract_A(S)$ and obtains an ABE private key $SK_S = (K, L, \{K_x\}_{x \in S})$.
  - When $ID \neq ID^*$, $\mathcal{B}$ sets the re-encryption key $RK_{I \to A} = (R_a, R_b, \{R_{ci}\}_{\rho(i) \in M'}, R_d, rk_1, rk_2\})$ as follows:
    Select $t', u' \in_R \mathbb{Z}_p$ and set

$$R_a = K \cdot g^{at'} \cdot SK^2_{ID} \cdot g^{u'} = K \cdot g^{at'} g^{\frac{-a^q z_2}{(ID-ID^*)}} \cdot g^{u'}.$$

    Select $\tau \in_R \mathbb{Z}_p$ and set

$$R_b = g^{\tau},$$
$$R_c = (g^{a z_1 (ID-ID^*)} g^{z_3})^{\tau},$$
$$R_d = e(g^a, g^{a^q})^{\tau}.$$

    Compute $rk_1 = L \cdot g^{t'}$ and for each $x \in S$,

$$rk_x = K_x \cdot h_x^{t'}.$$

  - When $ID = ID^*$, $\mathcal{B}$ chooses $t', u'' \in_R \mathbb{Z}_p$ and computes

$$R_a = K \cdot g^{at'} \cdot g^{u''} = K \cdot g^{at'} \cdot g^{u''}.$$

    Select $\tau \in_R \mathbb{Z}_p$ and set

$$R_b = g^{\tau}, \quad R_c = g^{z_3 \tau}, \; R_d = e(g^a, g^{a^q})^{\tau}.$$

    Compute $rk_1 = L \cdot g^{t'}$ and for each $x \in S$,

$$rk_x = K_x \cdot h_x^{t'}.$$

  Otherwise $S \models M^*$: If $\mathcal{B}$ already answers IBE private key for $ID$, $\mathcal{B}$ rejects. Otherwise, does as follows:
  - When $ID \neq ID^*$, $\mathcal{B}$ chooses $t'', u \in \mathbb{Z}_p$ and computes

$$R_a = g^{\alpha'} g^{at} g^{\frac{-a^q z_2}{(ID-ID^*)}} g^u.$$

    Select $\tau \in_R \mathbb{Z}_p$ and set

$$R_b = g^{\tau},$$
$$R_c = \left(g^{a z_1 (ID-ID^*)} g^{z_3}\right)^{\tau},$$
$$R_d = e\left(g^a, g^{a^q}\right)^{\tau}.$$

    Compute $rk_1 = g^{t''}, \quad \{rk_x = h_x^{t''}\}_{x \in S}$.
    *Remark:*

$$\begin{aligned} R_a &= g^{\alpha'} g^{at''} g^{\frac{-a^q z_2}{(ID-ID^*)}} g^u \\ &= g^{\alpha'+a^{q+1}} g^{at''} g^{\frac{-a^q z_2}{(ID-ID^*)}} g^{u-a^{q+1}} \\ &= g^{\alpha} g^{at} g^{at'} g^{\frac{-a^q z_2}{(ID-ID^*)}} g^{u_1} g^{u'} \\ &= K \cdot g^{at'} \cdot SK^2_{ID} \cdot g^{u'} \end{aligned}$$

    where $t + t' = t''$, $u = \frac{-a^q z_2}{(ID-ID^*)} + u_1$, $u_1 + u' = u - a^{q+1}$.
  - When $ID = ID^*$, $\mathcal{B}$ chooses $t, u \in \mathbb{Z}_p$ and computes $R_a = g^{\alpha'} g^{at} g^u$.
    Select $\tau \in_R \mathbb{Z}_p$ and set

$$R_b = (g^{z_3})^{\tau}, \quad R_c = g^{\tau}, \quad R_d = e(g^a, g^{a^q})^{\tau}.$$

    Compute $rk_1 = g^t$ and for each $x \in S$, $rk_x = h_x^t$.
    $\mathcal{B}$ returns $RK_{A \to I}$ to $\mathcal{A}$ and records the tuple ($S$,$ID$,$RK_{A \to I}$) in re-encryption key list (REKL).

**Challenge.** $\mathcal{A}$ submits two equal length plaintexts $\mathcal{M}_0, \mathcal{M}_1 \in \mathbb{G}_T$ and chooses which scheme to attack. $\mathcal{B}$ flips a coins $\beta$.
If $\mathcal{A}$ selects ABE scheme to attack, $\mathcal{B}$ builds the challenge ciphertext $CT^*_A = (C^*, C'^*, \{C^*_x, D^*_x\}_{\rho(x)^* \in M^*})$

$$C^* = \mathcal{M}_\beta \cdot T \cdot e(g^s, g^{\alpha'}), \qquad C' = g^s$$

$\mathcal{B}$ chooses $y'_2, \cdots, y'_{n^*}$ and the share the secret using the vector

$$\overrightarrow{v} = (s, sa + y'_2, sa^2 + y'_3, \cdots, sa^{n-1} + y'_{n^*}) \in \mathbb{Z}_p^{n^*}$$

$\mathcal{B}$ chooses $r'_1, \cdots, r'_\ell \in \mathbb{Z}_p$. For $i = 1, \cdots, n^*$, let $R_i$ as the set of all $k \neq i$ such that $\rho^*(i) = \rho^*(k)$ meaning the same attributes as row $i$.
$\mathcal{B}$ computes

$$D_i = g^{-r'_i} g^{-sb_i}$$

$$C_i = h^{r'_i}_{\rho^*(i)} \left( \prod_{j=2,\cdots,n^*} (g^a)^{M^*_{i,j} y'_j} \right) (g^{b_i \cdot s})^{-z_{\rho^*(i)}} \cdot \left( \prod_{k \in R_i} \prod_{j=1,\cdots,n^*} (g^{a^j \cdot s \cdot (b_i/b_k)})^{M^*_{k,j}} \right)$$

If $\mathcal{A}$ selects IBE scheme to attack, $\mathcal{B}$ outputs an IBE challenge ciphertext $CT^* = (C_1^*, C_2^*, C_3^*)$ corresponding to a target identity $ID^*$ as follows:

$$C_1^* = M_\beta \cdot T, \quad C_2^* = g^s, \ C_3^* = g^{sz_3}$$

**Phase 2.** Same as in Phase 1.

**Guess.** $\mathcal{A}$ outputs a guess $\beta' \in \{0, 1\}$. If $\beta' = \beta$ then $\mathcal{B}$ outputs 1 meaning $T = e(g, g)^{a^{q+1}s}$; otherwise, it outputs 0 to indicate $T$ is a random group element in $\mathbb{G}_T$.

*Theorem 2:* Suppose the decisional q-parallel BDHE assumption holds, the IBE→ABE type ES is IND-sCPA secure with a challenge matrix of size $\ell^* \times n^*$, where $\ell^*, n^* \leq q$.

*Proof:* The security of IBE→ABE type ES is similar to that of ABE→IBE type ES except the re-encryption key queries $Extract_{I\to A}(ID, S)$. Therefore, we just present the re-encryption key queries as follows.

$Extract_{I\to A}(S, ID)$ $\mathcal{A}$ queries the re-encryption key from identity $ID$ to attribute set $S$ as follows:

If $ID \neq ID^*$: $\mathcal{B}$ runs $Extract_I(ID)$ and obtains an IBE private key $SK_{ID} = (SK_{ID}^1, SK_{ID}^2)$.

- $S \not\models M^*$: $\mathcal{B}$ runs $Extract_A(S)$ and obtains an ABE private key $SK_S = (K, L, \{K_x\}_{x\in S})$. $\mathcal{B}$ uses $SK_{ID}$ and $SK_S$ to generate $RK_{I\to A} = (R_a, R_b, \{R_{ci}\}_{\rho(i)\in M'}, R_d, rk_1, rk_2\})$.
- $S \models M^*$: $\mathcal{B}$ chooses $t, t'', u' \in_R \mathbb{Z}_p$ and computes

$$R_a = SK_{ID}^1 \cdot (g^{az_1(ID-ID^*)} g^{z_3})^{u'} \cdot g^{\alpha'} g^{at} g^{at''}$$

*Remark:*

$$\begin{aligned} R_a &= SK_{ID}^1 \cdot (g^{az_1(ID-ID^*)} g^{z_3})^{u'} \cdot g^{\alpha'} g^{at} g^{at''} \\ &= SK_{ID}^1 \cdot (g^{az_1(ID-ID^*)} g^{z_3})^{u'} \cdot g^{\alpha'+a^{q+1}} g^{at} g^{a(t''-a^q)} \\ &= SK_{ID}^1 \cdot (g^{az_1(ID-ID^*)} g^{z_3})^{u'} \cdot g^{\alpha_1} g^{at} g^{a(t''-a^q)} \\ &= SK_{ID}^1 \cdot (g_1^{ID} h)^{u'} \cdot K \cdot g^{at'} \end{aligned}$$

$\mathcal{B}$ selects $\tau \in_R \mathbb{Z}_p$ and sets $R_b = g^\tau$.

Let $M^*$ be an $\ell \times n$ matrix. The algorithm first chooses a random vector $\vec{v^*} = (\tau, y_2^*, \cdots, y_n^*) \in \mathbb{Z}_p^n$. These values will be used to share the encryption exponent $\tau$.

For $i = 1$ to $\ell$, it calculates $\lambda_i^* = \vec{v^*} \cdot M_i^*$, where $M_i^*$ is the vector corresponding to the $i$th row of $M^*$. In addition, the algorithm chooses random $r_i^* \in \mathbb{Z}_p$ and computes

$$R_{ci} = \{C_i = g^{a\lambda_i^*} h_{\rho(i)}^{-r_i^*}, \quad D_i = g^{r_i^*}$$

$$R_d = \left(e(g^a, g^{a^q}) \cdot e(g, g)^{\alpha'}\right)^\tau$$

$\mathcal{B}$ chooses $\delta \in_R \mathbb{Z}_p$ and computes $rk_1 = sk_{ID}^2 \cdot g^{u'} \cdot g^\delta$, $\quad rk_2 = (g^{az_1(ID-ID^*)} g^{z_3})^\delta$. $\mathcal{B}$ returns $RK_{I\to A}$ to $\mathcal{A}$.

If $ID = ID^*$:

- $S \not\models M^*$: If $\mathcal{B}$ already answers ABE private key for $S$, $\mathcal{B}$ rejects. Otherwise, does as follows:
  $\mathcal{B}$ runs $Extract_A(S)$ to generate $K$, then it chooses $t'', u'' \in \mathbb{Z}_p$ and computes $R_a = g^{z_3(u'')} \cdot K \cdot g^{at''}$.
  *Remark:*

$$\begin{aligned} R_a &= g^{z_3 u''} \cdot K \cdot g^{at''} \\ &= g^{a^{q+1} z_1 z_2} g^{z_3(u+u')} \cdot K \cdot g^{a(t''-a^q z_1 z_2)} \\ &= g_2^{\alpha_2} (g_1^{ID^*} g_1^{-ID^*} g^{z_3})^{(u+u')} \cdot K \cdot g^{at'} \\ &= g_2^{\alpha_2} (g_1^{ID^*} h)^u (g_1^{ID^*} h)^{u'} \cdot K \cdot g^{at'} \end{aligned}$$

  where $t' = t'' - a^q z_1 z_2$.
  $\mathcal{B}$ generates $\{R_{ci}\}_{\rho(i)\in M^*}$ and $R_d$ as the case when $S \models M^*$ and $ID \neq ID^*$. $\mathcal{B}$ chooses $\delta \in \mathbb{Z}_p$ and computes $rk_1 = g^{u''+\delta}$, $rk_2 = g^{z_3\delta}$. $\mathcal{B}$ returns $RK_{I\to A}$ to $\mathcal{A}$.
- $S \models M^*$: $\mathcal{B}$ chooses $t'', u'' \in \mathbb{Z}_p$ and computes $R_a = g^{z_3(u'')} \cdot g^{\alpha'} g^{at} \cdot g^{at''}$.
  *Remark:*

$$\begin{aligned} R_a &= g^{z_3 u''} \cdot g^{\alpha'} g^{at} \cdot g^{at''} \\ &= g^{a^{q+1} z_1 z_2} g^{z_3(u+u')} \cdot g^{\alpha'+a^{q+1}} g^{at} \cdot g^{a(t''-a^q z_1 z_2 - a^q)} \\ &= g_2^{\alpha_2} (g_1^{ID^*} g_1^{-ID^*} g^{z_3})^{(u+u')} \cdot K \cdot g^{at'} \\ &= g_2^{\alpha_2} (g_1^{ID^*} h)^u (g_1^{ID^*} h)^{u'} \cdot K \cdot g^{at'} \end{aligned}$$

  where $t' = t'' - a^q z_1 z_2 - a^q$.
  $\mathcal{B}$ generates $\{R_{ci}\}_{\rho(i)\in M^*}$ and $R_d$ as the case when $S \models M^*$ and $ID \neq ID^*$. $\mathcal{B}$ chooses $\delta \in \mathbb{Z}_p$ and computes $rk_1 = g^{u''+\delta}$, $rk_2 = g^{z_3\delta}$. $\mathcal{B}$ returns $RK_{I\to A}$ to $\mathcal{A}$.

## V. EFFICIENCY ANALYSIS

### A. THEORETICAL ANALYSIS

In this subsection, we present the theoretical analysis of our construction in terms of computation, communication and storage complexity. In the analysis, we consider the following operations: $E_p$ denotes the computation in bilinear pairings, $E_e$ denotes the exponentiation computation, $|G_T|$ is the size of group $\mathbb{G}_T$, $|G_1|$ is the size of group $\mathbb{G}$, and $s$ is the number of user's attributes, respectively.

Table 2 presents the comparison of efficiency between two approaches, one being the naive decrypt-and-Re-Encrypt method, and the other being our ABE→IBE type ES. The naive solution is the one where a client first downloads the encrypted data in the format of ABE from cloud server, decrypts the data using ABE secret key, further re-encrypts the data under IBE format, and eventually uploads the resulting encryption to cloud. In the computational complexity, it can be seen from the table that the naive solution requires the client to consume linear cost in pairings, while ABE→IBE type ES only costs an $E_p$ on the client side (note the linear complexity is off-loaded to the cloud). Although the communication complexity of the two approaches is nearly identical, the storage cost incurred by ABE→IBE type ES gets rid of the linear requirement in $|G_1|$. Therefore, we can state that the new primitive designed in this paper outperforms the naive solution. We state that the complexity is reduced in our ES, which makes sense because the ES converts a complex encryption, ABE, into a much simpler one, IBE. However, this may not be the case for the conversion from IBE to ABE. From Table 3, we can see that the complexity of the two solutions is quite close; a few pairings are reduced in our IBE→ABE Type ES in the communication and computation costs. Therefore, we may state that the performance of

**TABLE 2. Comparison between Naive Decrypt-and-Re-Encrypt with our ABE→IBE Type ES.**

| | Naive Decrypt-and-Re-Encrypt | ABE→IBE Type ES |
|---|---|---|
| Computation | ABE.Dec+IBE.Enc: $(2+2s)E_p+6E_e$ | ES.ReKey (client side): $E_p+(3+s)E_e$ ES.ReEnc (cloud side): $2sE_p+3E_e$ |
| Communication | (ABE.CT+IBE.CT).Size $2\|G_T\|+(3+2s)\|G_1\|$ | (ES.ReKey).Size (from client to cloud) $\|G_T\|+(4+s)\|G_1\|$ |
| Storage | ABE.CT+IBE.CT $2\|G_T\|+(3+2s)\|G_1\|$ | ES.ReEnc.CT: $\|G_T\|+2\|G_1\|$ |

**TABLE 3. Comparison between Naive Decrypt-and-Re-Encrypt with our IBE→ABE Type ES.**

| | Naive Decrypt-and-Re-Encrypt | IBE→ABE Type ES |
|---|---|---|
| Computation | IBE.Dec+ABE.Enc: $3E_p+(3s+1)E_e$ | ES.ReKey (client side): $E_p+(5+3s)E_e$ ES.ReEnc (cloud side): $3E_p+3E_e$ |
| Communication | (ABE.CT+IBE.CT).Size: $2\|G_T\|+(3+2s)\|G_1\|$ | (ES.ReKey).Size (from client to cloud) $\|G_T\|+(4+2s)\|G_1\|$ |
| Storage | IBE.CT+ABE.CT: $2\|G_T\|+(3+2s)\|G_1\|$ | ES.ReEnc.CT: $2\|G_T\|+(2+s)\|G_1\|$ |

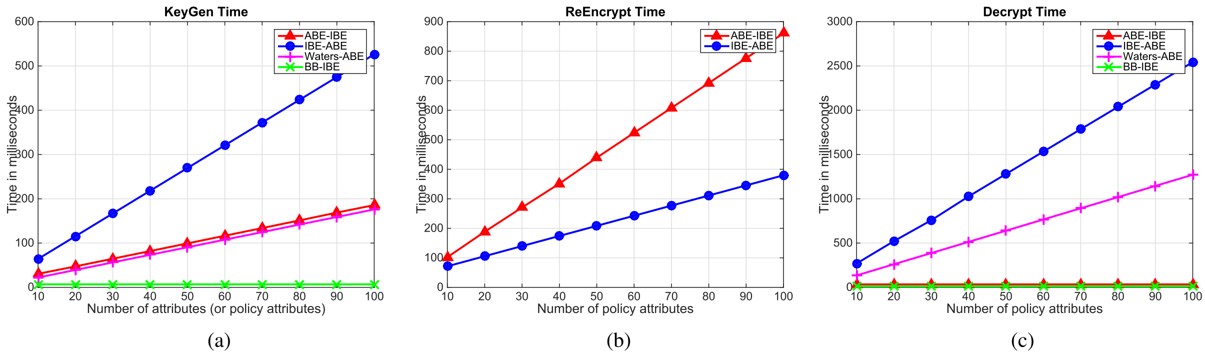



**FIGURE 1. Experimental analysis. (a) Keygen time. (b) Reencrypt time. (c) Decryption time.**

our solution is still a bit better than that of the naive solution w.r.t. the conversion from IBE to ABE.

### B. EXPERIMENTAL ANALYSIS

We make use of bilinear pairings $e : G_1 \times G_1 \rightarrow G_2$ to achieve the security level of 80 bits. To simulate the worst case, we generate ciphertext policies in the form of ($S_1$ and $S_2 \ldots$ and $S_l$) increasing from 10 to 100, where $S_i$ is an attribute. We repeat each instance 20 times and eventually take the average. The time in the figures is given in milliseconds. In the simulation, we use the widely studied cryptographic library MIRACL.[2] We run the simulation on an Intel I7-4770 processor with 3.40 GHz clock frequency and 4 GB RAM running Windows 7 operating system.

The simulation results (w.r.t. the time spent in computation) are shown in Fig 1(a), 1(b) and 1(c). In the figures, we let "ABE-IBE" denote the ABE→IBE Type ES (in Section III-B), "IBE-ABE" denote the IBE→ABE Type ES (in Section III-C), "BB-IBE" is the first construction in [9], respectively. The figure 1(a) shows the time spent in re-encryption key (w.r.t. ABE-IBE and IBE-ABE) and decryption key (w.r.t. Waters-ABE and BB-IBE) generation. IBE→ABE Type ES requires the longest time in the key preparation (nearly 0.52 s), while Waters-ABE and ABE→IBE Type ES share similar time complexity (around 0.18 s). The cost of time for BB-IBE is constant (approximately 0.01 s) because there is only one attribute, i.e. identity, embedded into the key. The figure 1(b) is about the complexity of re-encryption in our ESs. It can be seen that IBE-ABE (nearly 0.4 s) outperforms ABE-IBE (around 0.88 s). This is so because the re-encryption in the conversion from ABE to IBE requires the cost of pairings which is linear with the size of row matching set $I$ (while the re-encryption of IBE-ABE is in the cost of constant pairings). It is worth mentioning that the re-encryption burden in our ESs can be off-loaded to a cloud server. The decryption complexity comparison is shown in the figure 1(b). The cost of ABE-IBE and BB-IBE is constant (only using constant number of pairings), nearly 0.1s, while IBE-ABE suffers from the worst performance, 2.5 s (due to the fact that two linear groups of pairings are required in decryption). In general, from the simulation results shown in the Figures, we can state that the cost incurred by our ESs is acceptable in practice (with best case of $<1$ s and a worst case of 2.5 s).

## VI. CONCLUSIONS

In this paper, we have introduced encryption switching between IBE and ABE which is the first of its type in the literature. The security notion has been defined in the game-based framework. We have presented a concrete construction

[2]https://libraries.docs.miracl.com/miracl-user-manual/installation.

and meanwhile proved it to be CPA secure in the standard model under the decisional $q$-parallel BDHE assumption. The efficiency analysis has highlighted that our solution outperforms the download-and-re-encrypt conversion mode w.r.t. computation and communication cost. Finally, the simulation results have shown that the computational complexity in terms of re-encryption and decryption (in our construction) are in the acceptable range, e.g., around 0.9 s and 2.5 s for ABE→IBE re-encryption and decryption, respectively. In addition, some interesting open problems have emerged from this work, such as problem of how to shorten the re-encrypt and decrypt time in the case of ABE→IBE, and seek an approach to achieve simulation-based security.

## REFERENCES


[1] G. Couteau, T. Peters, and D. Pointcheval, "Encryption switching protocols," in *Advances in Cryptology—CRYPTO*, M. Robshaw and J. Katz, Eds., vol. 9814. New York, NY, USA: Springer, 2016, pp. 308–338.

[2] P. Paillier, "Paillier encryption and signature schemes," in *Encyclopedia Cryptography Security*, 2nd Ed., H. C. A. van Tilborg and S. Jajodia, Eds. New York, NY, USA: Springer, 2011, pp. 902–903.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, vol. 1984, Nov. 1984, pp. 47–53.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM CCS*, Oct. 2006, pp. 89–98.

[5] M. Portnoi and C. Shen, "Secure Zones: An Attribute-Based Encryption advisory system for safe firearms," in *Proc. IEEE Conf. Commun. Netw. Secur.*, Oct. 2013, pp. 397–398. doi: 10.1109/CNS.2013.6682746.

[6] M. Ambrosin, M. Conti, and T. Dargahi. (2010). *Andraben*. [Online]. Available: http://spritz.math.unipd.it/projects/andraben/files/

[7] T. Mizuno and H. Doi, "Hybrid proxy re-encryption scheme for attribute-based encryption," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, 2009, pp. 288–302.

[8] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Annu. Int. Cryptol. Conf.*, 2001, pp. 213–229.

[9] D. Boneh and X. Boyen, "Secure identity based encryption without random oracles," in *Proc. Annu. Int. Cryptol. Conf.*, 2004, pp. 443–459.

[10] B. Waters, "Efficient identity-based encryption without random oracles," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2005, pp. 114–127.

[11] C. Gentry, "Practical identity-based encryption without random oracles," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.*, 2006, pp. 445–464.

[12] C.-I. Fan, L.-Y. Huang, and P.-H. Ho, "Anonymous multireceiver identity-based encryption," *IEEE Trans. Comput.*, vol. 59, no. 9, pp. 1239–1249, Sep. 2010.

[13] X. Boyen and B. Waters, "Anonymous hierarchical identity-based encryption (without random oracles)," in *Proc. 26th Annu. Int. Cryptol. Conf.*, 2006, pp. 290–307.

[14] J. Kim, W. Susilo, M. H. Au, and J. Seberry, "Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 679–693, Mar. 2015.

[15] L. Wang, L. Wang, M. Mambo, and E. Okamoto, "Identity-based proxy cryptosystems with revocability and hierarchical confidentialities," *IEICE Trans.*, vol. 95-A, no. 1, pp. 70–88, 2012.

[16] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy*, May 2007, pp. 321–334. doi: 10.1109/SP.2007.11.

[17] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Proc. Int. Workshop Public Key Cryptogr.*, 2011, pp. 53–70.

[18] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Mar. 2013, pp. 463–474. doi: 10.1145/2508859.2516672.

[19] J. Ning, Z. Cao, X. Dong, L. Wei, and X. Lin, "Large universe ciphertext-policy attribute-based encryption with white-box traceability," in *Computer Security—ESORICS*. New York, NY, USA: Springer, 2014, pp. 55–72.

[20] J. Ning, X. Dong, Z. Cao, L. Wei, and X. Lin, "White-box traceable ciphertext-policy attribute-based encryption supporting flexible attributes," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 6, pp. 1274–1288, Jun. 2015.

[21] J. Ning, Z. Cao, X. Dong, and L. Wei, "White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively," *IEEE Trans. Dependable Secure Comput.*, vol. 15, no. 5, pp. 883–897, Oct. 2018.

[22] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017.

[23] J. Ning, Z. Cao, X. Dong, K. Liang, H. Ma, and L. Wei, "Auditable $\sigma$-time outsourced attribute-based encryption for access control in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 1, pp. 94–105, May 2018.

[24] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.*, 1998, pp. 127–144.

[25] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *Proc. Netw. Distrib. Syst. Secur. Symp., NDSS*, Feb. 2005, pp. 1–30. [Online]. Available: http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/ateniese.pdf

[26] R. Canetti and S. Hohenberger, "Chosen-ciphertext secure proxy re-encryption," in *Proc. ACM Conf. Comput. Commun. Secur.*, Jul. 2007, pp. 185–194.

[27] B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," *IEEE Trans. Inf. Theory*, vol. 57, no. 3, pp. 1786–1802, Mar. 2011.

[28] M. Green and G. Ateniese, "Identity-based proxy re-encryption," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, 2007, pp. 288–306.

[29] X. Liang, Z. Cao, H. Lin, and J. Shao, "Attribute based proxy re-encryption with delegating capabilities," in *Proc. 14th ACM Symp. Inf., Comput. Commun. Secur.*, Mar. 2009, pp. 276–286.

[30] L. Cheung and C. C. Newport, "Provably secure ciphertext policy ABE," in *Proc. ACM Conf. Comput. Commun. Secur.*, Feb. 2007, pp. 456–465.

[31] K. Liang *et al.*, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 10, pp. 1667–1680, Oct. 2014.

[32] T. Matsuo, "Proxy re-encryption systems for identity-based encryption," in *Proc. 1st Int. Conf. Pairing-Based Cryptogr.*, Tokyo, Japan, Jul. 2007, pp. 247–267.

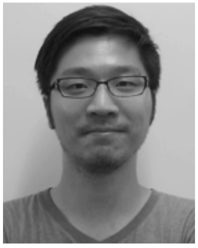


**KAI HE** received the M.S. and Ph.D. degrees from the College of Information Science and Technology from Jinan University in 2012 and 2016, respectively. Since 2017, she has been a Lecturer with the School of Computer and Network Security, Dongguan University of Technology. She has published several papers in refereed journals and conferences, such as IEEE TDSC, *Theoretical Computer Sciences*, AsiaCCS 2016 and ACISP 2016, and NSS 2016. Her research interests include cryptography and information security.

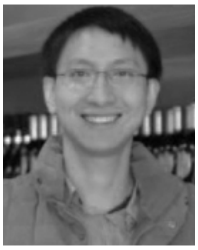


**YIJUN MAO** received the Ph.D. degree from Sun Yat-sen University, Guangzhou, in 2016. He is currently a Lecturer with the College of Mathematics and Informatics, South China Agricultural University, Guangzhou. His current research interests include artificial intelligence and information security.

**JIANTING NING** received the Ph.D. degree from the Department of Computer Science and Engineering, Shanghai Jiao Tong University, in 2016. He is currently a Research Fellow with the Department of Computer Science, National University of Singapore. His research interests include applied cryptography and cloud security, in particular, public key encryption, attribute-based encryption, and secure computation.



**KAITAI LIANG** received the Ph.D. degree from the Department of Computer Science, City University of Hong Kong, in 2014. He is currently a Lecturer (Assistant Professor) with the Department of Computer Science, University of Surrey, U.K. His research interests include applied cryptography and information security in particular, encryption, network security, big data security, privacy-enhancing technology, and security in cloud computing.



**XINYI HUANG** received the Ph.D. degree from the School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW, Australia, in 2009. He is currently a Professor with the Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, China. He has authored or co-authored more than 60 research papers in refereed international conferences and journals. His research interests include cryptography and information security. He has served as the Program/General Chair or Program Committee Member more than 40 international conferences. He is on the Editorial Board of the *International Journal of Information Security* (Springer).

**EMMANOUIL PANAOUSIS** received the B.Sc. degree in informatics and telecommunications from the University of Athens, Greece, in 2006, the M.Sc. degree in computer science from the Athens University of Economics and Business, Greece, in 2008, and the Ph.D. degree in mobile communications security from Kingston University London, U.K., in 2012. He was a Senior Lecturer in cybersecurity and privacy with the University of Brighton; an Invited Researcher with Imperial College London; a Postdoctoral Researcher with the Queen Mary University of London; and an R&D Consultant with Ubitech Technologies Ltd., Surrey Research Park. He is currently an Assistant Professor in secure systems with the University of Surrey. He has a series of publications in the broad field of developing game theoretic models to address various cybersecurity and privacy challenges. His current research interest includes game theory as applied to cybersecurity.

**GEORGE LOUKAS** received the Ph.D. degree in network security from Imperial College London. He is currently the Project Coordinator of H2020 EUNOMIA tackling disinformation online and a Principal Investigator of several other international research projects related to the security of smart homes, the Internet of Things, autonomous vehicles, and human-as-a-sensor systems. He has authored or co-authored more than 70 journals and conference publications. His book on cyber-physical attacks was included in ACM's top ten list in the computing milieux category of 2015. He is on the Editorial Board of the BCS *Computer Journal* and Elsevier's *Simulation Modelling Practice and Theory*.