Identity-Based Encryption Schemes – A Review

Boon Chian Tea[1], Muhammad Rezal Kamel Ariffin[1,2], Muhammad Asyraf Asbullah[*1,3]
[1]Institute for Mathematical Research (INSPEM), Universiti Putra Malaysia, 43400 UPM Serdang, Malaysia.
[2]Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Malaysia.
[3]Centre of Foundation Studies for Agricultural Science, Universiti Putra Malaysia, 43400 UPM Serdang, Malaysia.

***Abstract*—Identity-based encryption (IBE) allows a user to compute public key from arbitrary string such as name or email address as user's identity explicitly, thus provides a key-certificateless encryption platform while ensuring message confidentiality. In this paper, several identity-based encryption schemes are reviewed, ranging from the first practical well-known Boneh-Franklin IBE scheme based on pairing function to the recent IBE based on lattices. The aim of this review is to provide an extensive view and classification of these IBE schemes based on their setting, including underlying primitives in the parameter setup, fundamental security behind these schemes, comparative computational complexity and efficiency analysis. This review does not consider the variants of IBE such as hierarchical IBE, fuzzy IBE and those from the similar categories. Some current trends in IBE research and its implementation, along with some possible suggestions in designing new IBE schemes in the future are given as a conclusion of this review.**

Keywords—Identity-Based Encryption, Pairing Function, Multivariate, Trapdoor Subgroup, Lattice, Post-Quantum.

I. Introduction

The advancement in public key cryptography since 1976 has provided the world a new paradigm in achieving security in communication [1]. Via the use of a pair of different public-private keys (such as in well-known RSA Cryptosystem and Elliptic Curve Cryptography (ECC)), communicating parties are now able to encrypt and decrypt messages and then sent through insecure network channel. The benefit of this public key cryptography was however unable to be optimized effectively, as usability of public key cryptography are not as user-friendly as one might expect [2,3]. Making the situation worse, key management issue – (i) key storage capacity required to archive all the unique private keys for recovery purpose for distinct users are huge, and (ii) users' key certification and validation processes that are costly and length, resulting major drawbacks in its practical implementation.

Shamir in 1984 proposed the idea of generating public key using arbitrary string, such as user's name, email address or contact number, while explicitly computes the user's corresponding private key, i.e. the identity-based cryptography (IBC) to overcome the above-mentioned issues [4]. This new paradigm of encryption provides key-certificateless platform which effectively overcome the issue of key management by the server. However, it becomes a reality only after 16 years when Boneh and Franklin successfully designed a practical and secure identity-based encryption (IBE) scheme via the utilization of bilinear pairing on elliptic curve [5]. It is since then pairing function and IBE started to gain attention by many researchers and hence the birth of pairing-based cryptography.

The design of the IBE schemes does not limit to only using the pairing function, Clifford Cocks in the same year as Boneh and Franklin proposed an IBE scheme considering the quadratic residuosity which is number theoretic based as his underlying primitive [6]. His design features more efficient and cheaper computational cost than the Boneh-Franklin IBE but defeated at the produced ciphertext length (we will explain this further in the later section 5). Nevertheless, this opened alternative options for researchers to construct IBE scheme in different approaches rather than just using pairing function. Some researchers later considered the trapdoor subgroup over integer modulo composite number as their primitive [7,8].

As research progresses, in recent years, knowledge of linear algebra was also adapted in designing IBE schemes. One that is worth to mention to is the problem of lattices, since it has the potential to be one of the four (4) main areas that is currently expected to be post-quantum (besides hash-based, code-based and multivariate quadratic polynomial cryptography). Also, it involves only linear operations that is computational cost friendly and efficient, hence more focuses have been given in this area, especially in designing encryption type and signature type cryptosystems.

There are many surveys and reviews that have been done on IBE schemes, capturing the original design and its modification, along with some enhancement and improvement made. However, most of these papers either considered only IBE under the same primitive (pairing-based or lattice-based), comparing their own enhancement with the previous works, or included too many technical details and mathematics that are not suitable those who just started to get in touch with IBE. These do not imply that those papers are not good enough, rather it

Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 6 Issue 12, December - 2019, Special Issue

restricts the readers to only one-environment comparison. Readers who are expert and wish to focus on specific primitive may consider the articles due to Boyen [9] who discussed in detail about pairing-based IBE, and Hanaoka and Yamada [10] that surveyed the lattice-based IBE professionally.

A. Our Contribution

In this paper, we review several IBE schemes, ranging from the very first practical IBE scheme based on pairing function due to Boneh-Franklin, up to the current active design of IBE based on lattices. We currently do not consider IBE extensions such as Hierarchical IBE (HIBE) and some other variants such as Fuzzy IBE and similar categories [11,12,13]. Also, we try to simplify our content with lesser technical details, targeting those amateurs who wish to initiate their interest in researching the area of IBE.

The layout of this article is as follows. In section 2, we give preliminaries about the selected IBE schemes, considering their fundamental primitives in their designs. The selected IBE schemes and security model are presented in Section 3. Computation efficiencies and computational complexities are described in Section 4. We conclude our review in Section 5.

II. Preliminaries

We describe the fundamental mathematical tools in designing the selected IBE scheme in this section. There are four (4) different primitives that currently IBE schemes based on, namely bilinear pairing on elliptic curve, quadratic residuosity, trapdoor subgroup over integer modulo composite number and lattices.

A. Bilinear Pairing and Diffie-Hellman (DH) Variants

Pairing functions had been proposed since 1940 by few authors and its efficient computation algorithm in 1984 by Miller [14,15,16,17,18]. Confined to theoretical studies, their practical usage was only started in 1993 by Menezes et al. to attack the Elliptic Curve Cryptography (ECC) [19]. The first positive implementation of pairing was later in 2000s when Joux proposed a one-round tripartite key exchange using pairing function that successfully solved the multi party's key distribution problem, which initiated the research of pairing-based cryptography [20].

The definition of pairing function and its properties are given as follows.

Definition 1 [21]. (Pairing) Let $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ be finite cyclic groups. A pairing function is a map $\hat{e}: \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ that satisfies the following properties:

i. *Bilinearity*. For all $P, Q, R \in \mathbb{G}_1, \mathbb{G}_2$, $\hat{e}(P+Q, R) = \hat{e}(P, R) * \hat{e}(Q, R)$ and $\hat{e}(P, Q+R) = \hat{e}(P, Q) * \hat{e}(P, R)$.

ii. *Non-degeneracy*. For any $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, $\hat{e}(P, Q) \neq 1$.

iii. *Computability*. The pairing $\hat{e}$ is efficiently computable.

Furthermore, if $\mathbb{G}_1 = \mathbb{G}_2$, then it is called a symmetric pairing, otherwise asymmetric pairing.

The fundamental hardness behind pairing function lies on the difficulty of solving the Bilinear Diffie-Hellman Problem, which is a variant of the original Diffie-Hellman Problem (DHP) as defined as follows [22].

Definition 2. (Diffie-Hellman Problem) Let p be prime and g a generator of finite cyclic group $\mathbb{Z}_p^*$. The *Diffie-Hellman Problem* is the problem that given $g^a \pmod p$ and $g^b \pmod p$ for some integers $a, b \in \mathbb{Z}_p^*$, compute $g^{ab} \pmod p$.

Definition 3. (Decisional Diffie-Hellman Problem) Extended from Definition 2, the *Decisional DHP* is the problem that given two sets of (g, g^a, g^b, g^{ab}) and (g, g^a, g^b, g^c) for integer $c \in \mathbb{Z}_p^*$, determine whether $c \equiv ab \pmod p$.

Definition 4. (Bilinear Diffie-Hellman Problem) Let $\mathbb{G}$ and $\mathbb{G}_T$ be finite cyclic groups of prime order q and generator $P \in \mathbb{G}$. Let $\hat{e}: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ be a bilinear map. The *Bilinear DHP* is the problem that given the set of (P, aP, bP, cP) for some integers $a, b, c \in \mathbb{Z}_q^*$, compute $\hat{e}(P, P)^{abc}$.

Definition 5. (Decisional Bilinear Diffie-Hellman Problem) Extended from Definition 4, the Decisional *Bilinear DHP* is the problem that given two sets of (P, aP, bP, abP) and (P, aP, bP, cP) for integer $c \in \mathbb{Z}_q^*$, determine whether $c = ab$.

In next section we shall observe how these four (4) problems (alternatively known as assumptions) provide the security strength in their corresponding IBE schemes. Other than the four (4) problems described above, there are several other variants of Diffie-Hellman problem, such as q-Bilinear Diffie-Hellman Inversion problem which are not discussed here as the IBE schemes considered in this review do not rely on those. Readers who are interested may refer to [23, 24] on how these variants applied in IBE schemes of different designs.

B. Quadratic Residue, Jacobi Symbol and Quadratic Residuosity Problem

The idea of prime and composite numbers have been the core mathematics in cryptography since the revolution from symmetric cryptography to asymmetric cryptography in 1976. The Integer Factorization Problem (IFP) for instance, features the hardness of factoring into primes p and q given a composite number $N = pq$.

The following problem captures this core idea in its underlying primitive – the quadratic residuosity problem. We firstly define the concept of quadratic residue and Jacobi symbol [24].

Definition 6. (Quadratic Residue) Let a be integer, for positive integer N, a is called a *quadratic residue modulo* N if $\gcd(a, N) = 1$ and $x^2 \equiv a \pmod N$ for some integer x. Otherwise a is called a *quadratic nonresidue modulo* N.

Definition 7. (Jacobi Symbol) Let a be integer and N be positive odd integer such that $N = p_1 \dots p_k$ where p_i are odd primes, not necessarily distinct. The *Jacobi symbol* of $\left(\frac{a}{N}\right)$ is defined as

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_k}\right)$$

where $\left(\frac{a}{p_i}\right) \equiv a^{\frac{p_i - 1}{2}} \pmod{p_i}$ (known as *Legendre symbol*) satisfies the following conditions:

$$\left(\frac{a}{p_i}\right) = \begin{cases} +1, & \text{if } a \text{ is a quadratic residue mod } p_i \\ 0, & \text{if } p_i \text{ divides } a \\ -1, & \text{if } a \text{ is a quadratic nonresidue mod } p_i \end{cases}$$

Definition 8 [25]. (Quadratic Residuosity Problem) Extended from Definition 6, the *quadratic residuosity problem* is the problem that given integers a and N, where $N = pq$ with p, q two distinct unknown primes, determine whether a is a quadratic residue modulo N.

As explained earlier, if the integer factorization problem is easy, that is one can factor N into p and q, then determining whether an integer a is a quadratic residue becomes easy. However, there is no known efficient algorithm to defeat this problem currently, and this becomes the security strength to the proposal of Cocks IBE scheme in 2001 [6].

C. *Trapdoor Subgroup over Integer Modulo Composite Number,* $\mathbb{Z}_N^*$

There are many different types of trapdoor subgroup that are used to design IBE schemes, such as allowing a user to compute discrete logarithm modulo composite number N while remaining infeasibility for the user to factor N, which is due to the IBE scheme by Maurer and Yacobi in 1991 [26].

However, in this paper, we consider the trapdoor subgroup used by Park et al. in proposing their IBE scheme, as their design contains similar hard problem of trapdoor subgroup by Maurer and Yacobi, meanwhile exhibits similar setup as in other well-known IBE schemes [7].

Definition 9. (Trapdoor Subgroup) Let N be product of primes p, q such that $p = 2p_1 + 1$ and $q = 2q_1 + 1$ where p_1, q_1 are odd primes. Let order $\mathrm{ord}_N g$ be the least integer of x such that $g^x \equiv 1 \pmod N$ for generator g. Then a group $\mathbb{G}$ is called a *trapdoor subgroup* of $\mathbb{Z}_N^*$ when it is determined by (N, g), where $\mathrm{ord}_N g$ remains hidden and used as a 'trapdoor'.

Based on the Definition 9, the Euler-ϕ function for N is $\phi(N) = 4p_1q_1$. The IBE scheme designed using this trapdoor subgroup specifically construct a trapdoor subgroup $\mathbb{G}$ of order $\mathrm{ord}_N g = p_1q_1$ which is composite. It is easy to observe that if one can factor N efficiently, then one can solve to find p, q, followed by p_1, q_1 easily, this is indeed the integer factorization problem.

D. *Lattices and Learning With Errors (LWE)*

The first lattice-based cryptosystem started in 2008 by Gentry et al. in proposing their signature and IBE schemes [26]. The utilization of lattices in designing cryptosystem has gained so much attention in recent research due to its simplicity (which requires only linear operations and involves small integers). In addition, lattice-based cryptography is expected to be post-quantum, i.e. it is currently secure against quantum algorithm (quantum cryptanalysis). These huge advantages over other mathematical problems have led lattices to be one of the main focuses given in today's cryptography.

The core hardness of lattices rests on the difficulty of finding a Shortest Vector Problem (SVP) and Closest Vector Problem (CVP). However, the Learning with Errors (LWE) that was introduced by Regev in 2005 turned out to be the basis in most cryptographic constructions, especially in designing IBE schemes [27]. We outline the definitions of lattices and LWE as follows, leaving the SVP and CVP as it is not the main content of our discussion. Readers who are interested may refer to [28] for further readings about problems surrounding lattices.

Definition 10 [10]. (Lattices) For positive integers q, m, n, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n+m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^m$, the m-dimensional integer lattices $\Lambda_q^{\perp}(\mathbf{A})$ and $\Lambda_q^{\mathbf{u}}(\mathbf{A})$ are defined as

$$\Lambda_q^{\perp}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = \mathbf{0} \pmod q\}$$
$$\Lambda_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m : \mathbf{Ae} = \mathbf{u} \pmod q\}.$$

Definition 11. (Learning with Errors) Let $p = p(n) \le \mathrm{poly}(n)$ be some prime integers. Let the following list be 'equation with errors'

$$\langle s, \mathbf{a}_1 \rangle \approx_\chi b_1 \pmod p$$
$$\langle s, \mathbf{a}_2 \rangle \approx_\chi b_2 \pmod p$$
$$\vdots$$

where $s \in \mathbb{Z}_p^n$, $\mathbf{a}_i$ are chosen independently and uniformly from $\mathbb{Z}_p^n$, and $b_i \in \mathbb{Z}_p$. Then for each equation i such that $b_i = \langle s, \mathbf{a}_i \rangle + e_i$, where the error $e_i \in \mathbb{Z}_p$ is chosen independently according to probability distribution $\chi : \mathbb{Z}_p \to \mathbb{R}^+$ on $\mathbb{Z}_p$, the *Learning with Errors*, $\mathrm{LWE}_{p,\chi}$ denotes the problem of recovering s from these equations.

III. Identity-Based Encryption (IBE) Schemes and Security Model

Slightly different from traditional encryption schemes such as RSA and ECC where user's public and private keys are computed implicitly, these keys are computed explicitly in IBE scheme. In other words, user's public key is computed from some arbitrary string (usually identity ID) while its corresponding private key is computed using master secret that is kept by Private Key Generator (PKG). Therefore, an additional algorithm is needed for PKG to handle this private key generation – **Extraction** algorithm.

The conventional IBE scheme consists of quadruple randomized algorithms of (**Setup**, **Extract**, **Encrypt**, **Decrypt**) [24]:

i. **Setup**: On input of security parameter 1^n, output public system parameters $(param)$ and master secret (msk). The $param$ are to be publicized while msk is kept secret by Private Key Generator (PKG).

ii. **Extract**: On input of $param, msk$ and user's identity (ID), compute user's corresponding private key (decryption key).

iii. **Encrypt**: On input of $param$, user's ID and message M, output ciphertext C.

iv. **Decrypt:** On input of $param$, user's ID, user's private key and ciphertext C, output message M or abort $\perp$.

The correctness of IBE scheme remains the same as in any public key cryptosystem – with correct private key, ciphertext that is encrypted using the corresponding public key is decryptable.

For the security model in IBE, the definition of the notion of security is also slightly different from the traditional encryption scheme, since one must take account the possession of identities and their corresponding private keys by the adversary. Therefore, strengthening the definition is crucial to remain their security proofs' validity. We describe the security model (game) of an IBE scheme, following the model presented in Boneh-Franklin's paper [5].

i. *Setup*: The challenger takes the security parameter 1^n and runs the **Setup** algorithm. It output $param$ and keeps msk to itself.

ii. *Phase 1*: The adversary performs one of the following queries q_i:

   a) *Extraction queries* $\langle ID_i \rangle$. The challenger responds by running **Extract** algorithm to generate the private keys d_i corresponds to the public key $\langle ID_i \rangle$. It sends d_i to the adversary.

   b) *Decryption queries* $\langle ID_i, C_i \rangle$. The challenger responds by running **Extract** algorithm to generate the private keys d_i corresponds to ID_i. Next it runs **Decrypt** algorithm to decrypt the ciphertext C_i using the private key d_i, and sends the resulting plaintext to the adversary.

iii. *Challenge*: When adversary is ready to perform the challenge, it stops *Phase 1* and outputs two (2) plaintexts M_0 and M_1 and $ID \neq ID_i$ on which it wishes to attack. The challenger chooses a random bit $b \in \{0,1\}$ and sends $C = \text{Encrypt}(param, ID, M_b)$ to the adversary.

iv. *Phase 2*: The adversary issues more queries as in *Phase 1*:

   a) *Extraction queries* $\langle ID_i \rangle$. With the condition that $ID_i \neq ID$.

   b) *Decryption queries* $\langle ID_i, C_i \rangle$. With the condition that $\langle ID_i, C_i \rangle \neq \langle ID, C \rangle$.

v. *Guess*: The adversary finally outputs a guess $b' \in \{0,1\}$. The adversary wins the game if $b' = b$.

An IBE scheme is said to be secure against adaptive chosen ciphertext attack (IND-ID-CCA) if there does not exists polynomial time adversary that has non-negligible advantage, $\text{Adv}(\mathcal{A})$ against the challenger in the above security game, where

$$\text{Adv}(\mathcal{A}) = \left|\Pr[b = b'] - \frac{1}{2}\right|.$$

All the IBE schemes described in the following subsections used the above-mentioned game in their security proofs, with suitable adjustment due to standard and random oracle models. Readers can refer to each original paper for the complete proof and game descriptions.

A. *Pairing-Based IBE Schemes*

Soon after utilization of pairing function in constructive manner by Joux in 2000 [20], Boneh and Franklin successfully designed the very first practical and secure IBE scheme using the Weil pairing. Their design exhibits the Diffie-Hellman key exchange property via the computation of secret shared values using pairing function on elliptic curve, which is where the security of the scheme relies on.

We reviewed the two (2) most well-known IBE schemes based on pairing, the Boneh-Franklin and Boneh-Boyen IBE schemes. There are two versions of each of the schemes in their original papers, the CPA-secure and the CCA-secure versions. However, we consider the CCA-secure version in our review as it provides more powerful security notion which implies also the CPA security.

Before discussing the IBE schemes in details, we outline the general setup algorithm for $param$ generation. This algorithm helps to generate suitable curve and pairing function for practical use in setting up pairing-based IBE scheme.

Algorithm 1: General System Parameter Setup.

1) On input of security parameter 1^n, generates two random large primes p and q, such that $p | \#E(\mathbb{F}_q)$ and $p^2 \nmid \#E(\mathbb{F}_q)$, where $\#E(\mathbb{F}_q)$ indicates the number of points on elliptic curve E over $\mathbb{F}_q$.
2) Selects a random point (or generator) $P \in$

$E(\mathbb{F}_q)[p]$, and let $\mathbb{G} = \langle P \rangle$.

3) Let k be the smallest integer such that $p|q^k - 1$, i.e. the embedding degree of $E/\mathbb{F}_q$, generates pairing $\hat{e}: \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{F}_{q^k}^*$.
4) Let $\mathbb{G}_T = \langle \hat{e}(P, P) \rangle$.

The first IBE scheme due to Boneh and Franklin was proposed in 2001 [5]. Their scheme utilized the Weil pairing in a simple and straight forward manner, i.e. to compute the secret shared values as in Diffie-Hellman key exchange. The Boneh-Franklin IBE scheme was proven to be IND-ID-CCA secure via the random oracle model in which the random oracles are served by the hash functions H_1 and H_2 stated in the following algorithm. Their IBE scheme is changeable using Tate pairing instead of Weil by simply modifying the general parameter setup algorithm (Algorithm 1).

Algorithm 2: Boneh-Franklin IBE Scheme.

Setup:

1. Runs Algorithm 1.
2. Selects a random $s \in \mathbb{Z}_q^*$ and computes $P_1 = sP$.
3. Generates following hash functions:
   a) $H_1: \{0,1\}^* \rightarrow \mathbb{F}_p$
   b) $H_2: \mathbb{F}_{p^k} \rightarrow \{0,1\}^n$
   c) $H_3: \{0,1\}^n \times \{0,1\}^n \rightarrow \mathbb{F}_q$
   d) $H_4: \{0,1\}^n \rightarrow \{0,1\}^n$

   for some n.
4. Publicizes $\{p, n, P, P_1, H_1, H_2, H_3, H_4\}$ and keeps $\{s\}$.

Extract:

1. On user's ID, maps it to a point $Q = H_1(ID) \in E/\mathbb{F}_p$ of order q. This Q is user's public key.
2. Computes user's private key $d = sQ$.

Encrypt:

1. To encrypt message M using user's public key Q, sender chooses random $\sigma \in \{0,1\}^n$ and computes $r = H_3(\sigma, M)$.
2. Computes ciphertext tuple:
   a) $c_1 = rP$
   b) $c_2 = \sigma \oplus H_2(g^r)$ where $g = \hat{e}(rQ, P_1)$
   c) $c_3 = M \oplus H_4(\sigma)$

   where $\oplus$ denotes the exclusive-OR operation.
3. Sends $C = \{c_1, c_2, c_3\}$.

Decrypt:

1. Upon receiving $C = \{c_1, c_2, c_3\}$ and private key d, computes:
   a) $\sigma' = c_2 \oplus H_1(\hat{e}(d, c_1))$
   b) $M' = c_3 \oplus H_4(\sigma')$
   c) $r' = H_3(\sigma', M')$.
2. Checks whether $c_1 = r'P$. If not rejects the ciphertext, otherwise recover message M.

The second IBE scheme based on pairing after Boneh-Franklin was due to Boneh and Boyen in 2004 [30]. While Boneh-Franklin applied pairing function to compute secret shared value directly, Boneh-Boyen utilized the pairing in different fashion. Their design features the family of 'commutative blinding' scheme in which it involves computing ratio of two pairing values in the decryption process [24].

There are two (2) Boneh-Boyen IBE schemes proposed in the original article. In this case, we consider the first scheme which are selective ID-secure based on Decisional Bilinear Diffie-Hellman assumption without random oracle. It was presented in HIBE form but can easily be reduced to normal IBE scheme, we refer to [24] for the CCA-secure IBE version.

Also, in the **Setup** algorithm of the original Boneh-Boyen IBE schemes, there is no specific parameters given. Therefore, for this purpose we remain the same parameters as in Boneh-Franklin scheme since the elliptic curve chosen is one of the pairing-friendly types and works well when implementing it in the Boneh-Boyen IBE scheme.

Algorithm 3: Boneh-Boyen IBE Scheme.

Setup:

1. Runs Algorithm 1.
2. Selects a random $\alpha, \beta, \gamma \in \mathbb{Z}_p$ and computes $g^\alpha, g^\beta, g^\gamma$.
3. Computes public pairing value $v = \hat{e}(g^\alpha, g^\beta) = \hat{e}(g, g)^{\alpha\beta}$.
4. Generates following hash functions:
   a) $H_1: \{0,1\}^* \rightarrow \mathbb{F}_p$
   b) $H_2: \mathbb{F}_{p^k} \rightarrow \{0,1\}^n$
   c) $H_3: \mathbb{F}_{p^k} \times \{0,1\}^n \times \mathbb{F}_p \times \mathbb{F}_p \rightarrow \mathbb{Z}_p$

   for some n.
5. Publicizes $\{n, g, g^\alpha, g^\beta, g^\gamma, v, H_1, H_2, H_3\}$ and keeps $\{\alpha, \beta, \gamma\}$.

Extract:

1. On user's ID, maps it to an integer $z = H_1(ID) \in \mathbb{Z}_p$. This z is user's public key.
2. Randomly choose an integer $r \in \mathbb{Z}_p$, computes user's private keys $d_1 = g^{\alpha z r} g^{\alpha\beta r} g^{\gamma r}$ and $d_2 = g^r$.

Encrypt:

1. To encrypt message M using user's public key z, sender chooses random $s \in \mathbb{Z}_p$, computes $k = v^s$.
2. Compute ciphertext tuples:
   a) $c_1 = M \oplus H_2(k)$
   b) $c_2 = g^s$
   c) $c_3 = g^{\alpha z s} g^{\gamma s}$
   d) $c_4 = s + H_3(k, c_1, c_2, c_3)$.
3. Sends $C = \{c_1, c_2, c_3, c_4\}$.

Decrypt:

1. Upon receiving $C = \{c_1, c_2, c_3, c_4\}$ and private keys $\{d_1, d_2\}$, computes:
   a) $k' = \frac{\hat{e}(c_2, d_1)}{\hat{e}(c_3, d_2)}$
   b) $s' = c_4 - H_3(k', c_1, c_2, c_3)$.
2. Check whether $k = k' = v^{s'}$ and $c_1 = g^{s'}$, if not rejects the ciphertext.
3. Recover message $M = c_1 \oplus H_2(k')$.

The main core security behind these pairing-based IBE schemes lies on the assumptions of Diffie-Hellman (as in Definition 2) and Decisional Bilinear Diffie-Hellman (as in Definition 5). As outlined in the above two (2) schemes, the decryption of the ciphertexts requires the receiver to firstly computes the secret shared values via the pairing function, that is in the first step in both IBEs' decryption procedure. We illustrate this statement further using Boneh-Franklin IBE scheme:

$$\hat{e}(d, c_1) = \hat{e}(sQ, rP) = \hat{e}(Q, P)^{sr} = \hat{e}(rQ, sP) = \hat{e}(rQ, P_1).$$

If an adversary can compute $\hat{e}(Q, P)^{sr}$ from both points P and Q in polynomial time, he has then successfully defeated the Diffie-Hellman assumption. On the other hand, if the adversary can compute $\hat{e}(Q, P)^x = \hat{e}(Q, P)^{sr}$ for some integer x, then he is able to determine whether $x = sr$, which is precisely the Decisional Bilinear Diffie-Hellman assumption.

The IBE schemes by Boneh-Franklin and Boneh-Boyen are now proposed to be standardized by National Institute for Standard and Technology (NIST), specified in the IEEE P1363.3, along with another two (2) IBE schemes of Sakai-Kasahara Key Encapsulate Mechanisms (KEM) and Boneh-Boyen Key Encapsulate Mechanism [31].

Other than these two (2) IBE schemes above, there are several pairing-based IBE published after them, for instance Sakai-Kasahara IBE scheme in which the 'exponent inversion' type of pairing is used, i.e. its security is due to q-Bilinear Diffie-Hellman Inversion assumption [23].

B. IBE Scheme Based on Quadratic Residuosity

Proposed by Cocks in 2001 right after the IBE by Boneh-Franklin, this IBE scheme was designed utilizing different approach, i.e. based on the difficulty of solving the Quadratic Residuosity problem.

The Cocks IBE scheme is described as follows [6].

Algorithm 4: Cocks IBE Scheme.

Setup:
1. On input of security parameter 1^n, generates two random large primes p, q such that $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$.
2. Computes $N = pq$.
3. Generates a hash function $H: \{0,1\} \to \mathbb{Z}_N$.
4. On input of user's ID, compute user's public key $a = H(ID)$ such that the jacobi symbol $\left(\frac{a}{N}\right) = +1$.
5. Publicizes $\{N, a, H\}$ and keeps $\{p, q\}$.

Extract:
1. On user's public key $H(ID)$, computes user's private key $r \equiv a^{\frac{\phi(N)+4}{8}} \pmod N$.

Encrypt:
1. To encrypt message M, encodes M as $m = (-1)^M$.
2. Selects random t_1 and t_2 such that $\left(\frac{t_1}{N}\right) = \left(\frac{t_2}{N}\right) = m$.
3. Computes ciphertexts
$$c_1 \equiv \left(t_1 + \frac{a}{t_1}\right) \pmod N$$
$$c_2 \equiv \left(t_2 - \frac{a}{t_2}\right) \pmod N.$$
4. Sends ciphertexts $C = \{c_1, c_2\}$.

Decrypt:
1. Upon receiving ciphertexts $C = \{c_1, c_2\}$ and private key r, computes
$$r^2 \equiv \begin{cases} +a, & \text{then let } C = c_1 \\ -a, & \text{then let } C = c_2. \end{cases}$$
2. Computes the encoded message bit
$$m = \left(\frac{C + 2r}{N}\right) = \begin{cases} -1 & \text{, then let } m = 0 \\ +1 & \text{, then let } m = 1. \end{cases}$$

The Cocks IBE scheme shows that for each bit of the message (plaintext) encrypted, two (2) bits of corresponding ciphertexts are produced (step 3 in **Encrypt**). Since it is unknown whether a or $-a$ is a square root modulo N, receiver who possesses the private key can easily verify whether $r^2 \equiv +a \pmod N$ or $r^2 \equiv -a \pmod N$ and hence able to perform decryption on the ciphertext successfully. This is indeed the hardness of the quadratic residuosity.

Besides, the security of Cocks IBE scheme also related to the difficulty of integer factorization problem (in which the RSA cryptosystem security based). As $N = pq$, if the adversary can find the factors of p and q, he can next solve the quadratic residuosity problem (following Definition 7) and determine which ciphertext C should be chosen. Hence successfully decrypting the ciphertext to recover the message.

C. IBE Scheme Based on Trapdoor Subgroup

As explained in the previous section, we considered the IBE scheme based on trapdoor subgroup due to Park et al., which defined the trapdoor subgroup differently compared to the definition by Maurer and Yacobi [7,26]. However, both definitions presented the same core idea – the infeasibility of factoring composite integer that leads to the security of the Discrete Logarithm problem in computing the secret shared values.

We present the CCA-secure version of the IBE scheme based on trapdoor subgroup by Park et al. as follows [7].

Algorithm 5: IBE Scheme Based on Trapdoor Subgroup.

Setup:
1. On input of security parameter 1^n, generates two safe primes $p = 2p_1 + 1$ and $q = 2q_1 + 1$ for primes p_1, q_1.
2. Computes $N = pq$.
3. Selects a random generator $g \in \mathbb{Z}_N^*$ such that $\mathrm{ord}_N g = p_1 q_1$.
4. Chooses a random $x \in \mathbb{Z}_{\mathrm{ord}_N g}$ and sets $g_1 \equiv g^x \pmod N$.
5. Generates following hash functions:
   a) $H_1: \{0,1\}^* \to \{0,1\}^l$, where $l < \log(ord_N g)$
   b) $H_2: \mathbb{Z}_N \to \{0,1\}^{\delta+\theta}$
   c) $H_3: \{0,1\}^* \to \{0,1\}^{\lceil \log N \rceil}$.
6. Publicizes $\{N, g, g_1, H_1, H_2, H_3\}$ and keeps

$\{x, \mathrm{ord}_N g\}$.

Extract:

1. On user's ID, computes $a = H_1(ID)$.
2. Checks whether $\gcd(x + H_1(ID), \mathrm{ord}_N g) = 1$. If do, computes user's private key d such that $d(x + H_1(ID)) \equiv 1 \pmod{\mathrm{ord}_N g}$. Else abort.

Encrypt:

1. To encrypt message $M \in \{0,1\}^\delta$ with user's public key a, selects a random $\rho \in \{0,1\}^\theta$ and computes $s = H_3(M, ID, \rho) \in \{0,1\}^{\lceil \log N \rceil}$.
2. Computes ciphertexts:
   a) $c_0 \equiv g^s \pmod N$
   b) $c_1 \equiv (g_1 g^a)^s \pmod N$
   c) $c_2 = H_2(c_0) \oplus (M \parallel \rho) \in \{0,1\}^{\delta+\theta}$.
3. Sends ciphertext pair $C = \{c_1, c_2\}$.

Decrypt:

1. Upon receiving ciphertext $C = \{c_1, c_2\}$ and private key d, computes:
   a) $c_0' \equiv c_1^d \pmod N$
   b) $(M' \parallel \rho') = H_2(c_0') \oplus c_2$
   c) $s' = H_3(M', ID, \rho')$
2. Checks whether $c_1 \equiv (g_1 g^a)^{s'} \pmod N$. If not rejects the ciphertext, otherwise recover message M.

The main attraction in the IBE scheme by Pak et al. is the infeasibility of finding the secret trapdoor – the $\mathrm{ord}_N g$. If such problem can be solved efficiently, then it implies that factoring the modulus N is easy, since an adversary knows the $\mathrm{ord}_N g = p_1 q_1$ that can next use these primes to solve for p and q.

Besides the hardness of finding $\mathrm{ord}_N g$, the discrete logarithm assumption is another attention-drawing point. Since solving discrete logarithm is equivalent to solving the integer factorization problem, if x can be found, then by the congruence relation $d(x + H_1(ID)) \equiv 1 \pmod{\mathrm{ord}_N g}$, one can efficiently find the private key d and next decrypt the ciphertext intercepted easily [7].

D. Lattice-Based IBE Scheme

The very first IBE scheme based on lattices was proposed by Gentry et al. in 2008. Rely on the hardness of solving the LWE problem, they designed several cryptosystems in the same paper, that are signature, encryption and IBE schemes. However, unlike other designs, Gentry et al. used the dual cryptosystem in constructing their IBE scheme.

Before giving the details of the IBE scheme, the following lemmas provides the core constructions of the scheme in the **Setup** and **Extract** algorithms [10].

Lemma 1. There is an efficient randomize algorithm that given $\mathrm{TrapGen}(1^n, 1^m, q) \to (\mathbf{A}, \mathbf{T_A})$, that when $m \geq 6n\lceil \log q \rceil$, outputs a full rank matrix $\mathbf{A} \in \mathbb{Z}_q^{n+m}$ and a basis $\mathbf{T_A} \in \mathbb{Z}^{m+m}$ for $\Lambda_q^\perp(\mathbf{A})$ such that $\mathbf{A}$ is $\mathrm{negl}(n)$-close to uniform $\|\mathbf{T_A}\| = \mathcal{O}(\sqrt{n \log q})$ with all but negligible probability in n.

Lemma 2. (GVP-Sampling) There is a probabilistic polynomial time (PPT) algorithm that given $\mathbf{A} \in \mathbb{Z}_q^{n+m}$, $\mathbf{T_A} \in \mathbb{Z}^{m+m}$, $\sigma > \|\mathbf{T_A}\| \cdot \omega(\sqrt{\log n})$ and $\mathbf{u} \in \mathbb{Z}_q^n$, and outputs a sample from the distribution statistically close to $D_{\Lambda^{\mathbf{u}}(\mathbf{A}),\sigma}$, where $D_{\Lambda^{\mathbf{u}}(\mathbf{A}),\sigma}$ is the discrete Gaussian distribution over Λ with parameter σ. Such algorithm is denoted by $\mathrm{GVPSamp}$.

We now describe the lattice-based IBE scheme based on Gentry et al. in [28] but refer to the simplified version from Hanaoka dan Yamada as follows [10].

Algorithm 6: IBE Based on Lattices.

Setup:

1. On input of security parameter 1^λ, runs $\mathrm{TrapGen}(1^n, 1^m, q) \to (\mathbf{A}, \mathbf{T_A})$.
2. Generates hash function $H: ID \to \mathbb{Z}_q^n$ for user's identity.
3. Publicizes $\{\mathbf{A}, H\}$ and keeps $\{\mathbf{T_A}\}$.

Extract:

1. On user's ID, computes $\mathbf{u} = H_1(ID)$.
2. Computes user's private key
$$\mathbf{e} \leftarrow \mathrm{GVPSamp}(\mathbf{A}, \mathbf{T_A}, \sigma, \mathbf{u})$$
   where $\mathbf{e} \in \mathbb{Z}^m$ is a short vector satisfies $\mathbf{Ae} = \mathbf{u}$.

Encrypt:

1. To encrypt message $M \in \{0,1\}$, samples random $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $x_0 \leftarrow D_{\mathbb{Z},\alpha}$, and $\mathbf{x} \leftarrow D_{\mathbb{Z}^m,\alpha}$.
2. Computes ciphertexts:
   a) $c_1 = \mathbf{s}^\intercal \mathbf{u} + x_0 + M \cdot \left\lfloor \frac{q}{2} \right\rfloor$
   b) $\mathbf{c}_2^\intercal = \mathbf{s}^\intercal \mathbf{A} + \mathbf{x}^\intercal$.
3. Sends ciphertext $C = \{c_1, \mathbf{c}_2^\intercal\}$.

Decrypt:

1. Upon receiving ciphertext $C = \{c_1, \mathbf{c}_2^\intercal\}$ and private key $\mathbf{e}$, computes $w = c_1 - \mathbf{c}_2^\intercal \mathbf{e} \pmod q$.
2. Checks whether w is closer to $\frac{q}{2}$ than to 0 over $\mathbb{Z}_q$. If not rejects the ciphertext, otherwise recover message M.

Gentry et al. in their work proved that their scheme is secure under random oracle model via the assumption of LWE. The standard model was only given Cash et al. in 2010 [32]. The underlying security assumption of Gentry et al. IBE scheme is that, if an adversary intercepted ciphertext $C = \{c_1, \mathbf{c}_2^\intercal\}$, specifically $\mathbf{c}_2^\intercal = \mathbf{s}^\intercal \mathbf{A} + \mathbf{x}^\intercal$, then it is computationally infeasible for the adversary to distinguish the two (2) given sets of distributions between $(\mathbf{A}, \mathbf{s}^\intercal \mathbf{A} + \mathbf{x}^\intercal)$ and $(\mathbf{A}, \mathbf{v}^\intercal)$ where $\mathbf{v} \leftarrow \mathbb{Z}_q^m$, and this implies the difficulty of recovering $\mathbf{s}$ as well [10].

Utilizing LWE problem is not the only way to design a lattice-based IBE scheme, another interesting method that worth its mentioned is the IBE scheme proposed using the NTRU lattices. However, we do not outline the NTRU Lattice-based IBE scheme and readers who are interested may consider referring [33] for more details.

We summarize all the five (5) IBE schemes discussed above in the following Table I.

TABLE I. SUMMARY OF SELECTED IBE SCHEMES.

IBE Scheme	Primitive	Security Assumption	CCA Security	Additional Notes
Boneh-Franklin	Pairing on Elliptic Curve	Decisional Bilinear Diffie-Hellman	Yes	Standardized in IEEE P1363.3 by NIST [31]
Boneh-Boyen	Pairing on Elliptic Curve	Decisional Bilinear Diffie-Hellman	Yes	Standardized in IEEE P1363.3 by NIST [31]
Cocks	Quadratic Residue	Quadratic Residuosity	Yes	-
Park et al.	Trapdoor Subgroup over $\mathbb{Z}_N^*$	Trapdoor Subgroup, Integer Factorization	Yes	-
Gentry et al.	Learning with Errors	Learning with Errors	Yes	Expected to be post-quantum [10]

IV. COMPARATIVE ANALYSIS

In this section, we discuss in a general perspective about the computation efficiency and computational complexity of all the five (5) IBE schemes described above. Readers should take note that the exact computation of the IBE schemes are varied from one to another, since each scheme consider groups (finite or arbitrary groups) and functions (hash and pairing) in different setting.

A. *Computation Efficiency*

We provide the notations prior to the discussion of the computation efficiency as follows:

i. H denotes hash function.
ii. $\mathbb{G}$ denotes group.
iii. L denotes lattice (matrix/vector).
iv. D denotes Gaussian distribution.
v. P denotes pairing computation.
vi. h denotes hashing.
vii. E denotes modulo exponentiation.
viii. Mod denotes modulo addition/subtraction.
ix. A denotes addition/subtraction.
x. M denotes multiplication/division.
xi. $\oplus$ denotes exclusive-OR (XOR) operation.

The computation efficiency of all the reviewed IBE schemes are summarized in the following Table II.

TABLE II. SUMMARY OF COMPUTATION EFFICIENCY OF SELECTED IBE SCHEMES.

IBE Scheme	Setup	Extraction	Encryption	Decryption
Boneh-Franklin	$3\mathbb{G}, 4H, 1A$	$1h, 1A$	$3h, 2E, 2\oplus, 1P$	$3h, 1P, 2\oplus, 1A$
Boneh-Boyen	$3\mathbb{G}, 3H, 3E, 1P$	$1h, 4E, 2M$	$2h, 4E, 1\oplus, 1M, 1A$	$2h, 2P, 1\oplus, 1A, 3E$
Cocks	$1H, 1h, 1M$	$1E, 2M, 3A$	$4E, 2A$	$3E, 1A, 1M$
Park et al.	$3H, 1E, 4M, 2A$	$1h, 1I, 1A$	$2h, 3E, 1\oplus, 1M$	$2h, 3E, 1\oplus, 1M$
Gentry et al.	$2L, 1H$	$2L, 1h$	$1L, 2D, 3M, 3A$	$1M, 1A, 1\mathrm{Mod}$

From the summary above, it is interestingly noticeable that among the five (5) selected IBE schemes, lattice-based by Gentry et al. has simpler operations (as explained in previous section) in both encryption and decryption procedures, as they mainly involve only linear lattice multiplications and additions. Therefore, one could conclude that overall this IBE scheme is more efficient than the other four (4) IBE schemes.

IBE schemes due to Boneh-Franklin and Boneh-Boyen may seem having less advantage among the selected schemes, due to their expensive pairing operations in the encryption and decryption processes. Though these two (2) are well recognized as practical and secure IBE schemes, as many studies have been performed (including cryptanalysis by experts) on the IBE schemes and the underlying strong-established hard problem (Diffie-Hellman assumption). Such strong evidence and security proof granted these IBE schemes strength and they are now under the standardization by NIST.

Cocks' IBE scheme at first sight may seem to have more advantage over pairing-based IBE as it does not involve expensive pairing computations and was proposed at the same year as Boneh-Franklin in 2001. However, due to its longer ciphertext length produced for equivalent security strength, i.e. for each bit of message in Cock's IBE scheme, two (2) bits of ciphertext are produced. For 112-bit security, Cocks IBE would need to channel 458,752 bits of ciphertext which is extremely lengthy, and this is obviously impractical for implementation purpose [24].

B. *Computational Complexity*

Like many cryptographic schemes, the security of IBE schemes rely on the hardness assumption of solving certain mathematical problem, as defined in Section 2. The assumption stated here referred to the infeasibility of current classical computing power to output solutions to those problem efficiently. For instance, to solve the integer factorization problem when $N = pq$ for both p and q large primes, this problem requires exponential-time algorithm to solve it efficiently, which is currently impossible in polynomial-time algorithm in classical computer.

The above situation described is the study of complexity theory. We put the popular three (3) classes in complexity theory that are widely discussed in the following definitions, referring to [34].

Definition 12. ($\mathcal{P}$-class) The class of problems that are solvable in polynomial time by a Deterministic Turing Machine (DTM), i.e. in polynomial time.

Definition 13. ($\mathcal{NP}$-class) The class of problems that are solvable in polynomial time by a Non-Deterministic Turing Machine (NDTM).

Definition 14. ($\mathcal{EXP}$-class) The class of problems that are solvable by DTM in time bounded by 2^{n^i}, i.e. in exponential time.

Besides the three (3) main classes, there are algorithms that grow faster than polynomial time algorithm but significantly smaller than exponential time algorithm, we called such class as sub-exponential time algorithm.

The Boneh-Franklin and Boneh-Boyen IBE schemes which based on pairing on elliptic curve has the core problem of Elliptic Curve Discrete Logarithm Problem (ECDLP), that given points P and $Q = nP$, find the integer n. There are few algorithms that can be used to solve ECDLP, such as Pohlig-Hellman, Baby-step Giant-step, and the Pollard's ρ algorithms. Currently the Pollard's ρ algorithm is the best-known (fastest) algorithm to solve ECDLP over finite prime field $\mathbb{F}_p$ and has the complexity of $\mathcal{O}(\sqrt{p})$ which is exponential [21].

For the IBE scheme by Cocks which used quadratic residue and IBE scheme by Park et al. which utilized trapdoor subgroup over $\mathbb{Z}_N^*$, the common core problem behind these two (2) schemes is the integer factorization problem (IFP) of factoring N into primes p and q. There are few algorithms that can be used to solve this IFP – the Pollard $(p-1)$, Coppersmith method, continued fraction, quadratic sieve and number field sieve methods, to name a few. Among the listed methods, the general Number Field Sieve (NFS) is the fastest known method to the current stage in solving the IFP which has the complexity of $\mathcal{O}\left(\exp\left(\sqrt[3]{\frac{64}{9}}\sqrt{\log n}\sqrt[3]{(\log\log n)^2}\right)\right)$ that is sub-exponential. Even though there is another core problem lies in the Park et al. IBE scheme – the Discrete Logarithm Problem (DLP), the fastest algorithm for solving DLP which is index calculus method has the complexity of $\mathcal{O}\left(\exp\left(\sqrt{2}\sqrt{\log n \, \log\log n}\right)\right)$ which is also sub-exponential, but is relatively larger than the NFS method, so it is comparatively best to consider NFS over index calculus when cryptanalyzing Park et al. IBE scheme.

Unlike the rest of the selected IBE scheme which utilized the mathematical hard problems that have unique solution, the lattice-based IBE scheme by Gentry et al. used the random sampling for lattice $\mathbf{A}$ and therefore the complexity analysis is differ from those of conventional one. Since there are many different complexities for different cases under LWE, following [27], the best way to generalize the complexity is to take the upper bound which is $\mathcal{O}(n^k)$ for some integer k that is exponential. Since currently there is no known efficient algorithm to solve the LWE problem in general even in the presence of quantum computer, lattice-based IBE is expected to be post-quantum secure.

TABLE III. COMPUTATIONAL COMPLEXITY OF SELECTED IBE SCHEMES.

IBE Scheme	Fundamental Primitive	Core Problem	Fastest Algorithm	Computational Complexity
Boneh-Franklin	Pairing on Elliptic Curve	Elliptic Curve Discrete Logarithm Problem	Pollard's ρ Method	$\mathcal{O}(\sqrt{p})$
Boneh-Boyen	Pairing on Elliptic Curve	Elliptic Curve Discrete Logarithm Problem	Pollard's ρ Method	$\mathcal{O}(\sqrt{p})$
Cocks	Quadratic Residue	Integer Factorization Problem	Number Field Sieve	$\mathcal{O}\left(\exp\left(\sqrt[3]{\frac{64}{9}}\sqrt{\log n}\sqrt[3]{(\log\log n)^2}\right)\right)$
Park et al.	Trapdoor Subgroup over $\mathbb{Z}_N^*$	Integer Factorization Problem and Discrete Logarithm Problem	Number Field Sieve	$\mathcal{O}\left(\exp\left(\sqrt[3]{\frac{64}{9}}\sqrt{\log n}\sqrt[3]{(\log\log n)^2}\right)\right)$
Gentry et al.	Learning with Error	Lattice	N/A	$\mathcal{O}(n^k)$

The above Table III summarizes the IBE schemes and their corresponding primitive, core problem, the fastest known algorithm for solving the core problem and their corresponding computational complexity. Once again it should be noted that the fastest known algorithm indicates the best method to solve the hard problem lied in the IBE scheme.

V. Conclusion and Future Work

In this article, we have reviewed several IBE schemes designed using various mathematical problems – pairing function on elliptic curve, quadratic residue, trapdoor subgroup over integer modulo composite number, and learning with errors on lattices. All these schemes exhibit different approaches in their setup, as well as their corresponding computation efficiencies and computational complexities. One scheme may be efficient and acquire advantage in generating public parameters while another scheme has advantage of shortest ciphertext over the rests.

The security of IBE are based on current well-recognized hard mathematical problems, i.e. solving these problems using current best classical computing power is infeasible. While the idea of quantum computer may soon be a reality, alongside with the introduction of Shor's and Grover's quantum algorithms [35,36,37] that can break most of the current public key cryptography including the IBE schemes, research on post-quantum scheme should be given more focus. As readers may have noticed, the IBE scheme based on lattice features such potential in surviving against quantum cryptanalysis, since it is one of the mathematical tools that is still inefficient to be cryptanalyzed even under quantum algorithms.

Besides relying solely on lattices, other post-quantum candidates can be exploited, such as multivariate quadratic polynomial in designing novel IBE schemes. This could be another potential research area in the future, in line with enhancing and strengthening current schemes to achieve better efficiency and usability.

Acknowledgment

The present research was partially supported by the Putra Grant with Project Number GP/2017/9552200.

References

[1] W. Diffie, and M. Hellman, "New directions in cryptography," in IEEE Trans. Inf. Theor., vol. 22(6), pp. 644-654, 1976.

[2] A. Whitten, and J.D. Tygar, "Why Johnny Can't Encrypt," Proceedings of the 8th USENIX Security Symposium, Washington, D.C., Aug. 23–36, 1999, pp.169-184.

[3] S. Sheng, L. Broderick, C.A. Koranda, and J.J. Hyland, "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software," in Proceedings of the 2006 Symposium on Usable Privacy and Security, Pittsburgh, PA, July 12-14, 2006.

[4] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," in Blakley G.R., Chaum D. (eds.) Advances in Cryptology - CRYPTO1984, LNCS, vol. 196, pp. 47-53. Springer, Berlin, Heidelberg, 1985.

[5] D. Boneh, and M. Franklin, "Identity-Based Encryption from the Weil Pairing," in Kilian J. (eds.) Advances in Cryptology - CRYPTO 2001, LNCS, vol. 2139, pp. 213-229. Springer, Berlin, Heidelberg, 2001.

[6] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues," in Honary B. (eds) Cryptography and Coding: Cryptography and Coding 2001, LNCS, vol. 2260, pp. 360-363. Springer, Berlin, Heidelberg, 2001.

[7] J.H. Park, K. Lee, and D.H. Lee, "Efficient Identity-Based Encryption and Public-Key Signature from Trapdoor Subgroups," IACR Cryptology ePrint Archive, pp. 500, 2016.

[8] J. Liu, and L. Ke, "New Efficient Identity Based Encryption Without Pairings," in Journal of Ambient Intelligence Humanized Computing, vol. 10(4), pp. 1561-1570, 2019.

[9] X. Boyen, "A Tapestry of Identity-Based Encryption: Practical Frameworks Compared," in International Journal of Applied Cryptolgraphy, vol. 1(1), pp. 3-21, 2008.

[10] G. Hanaoka, and S. Yamada, "A Survey on Identity-Based Encryption from Lattices," in: Takagi T., Wakayama M., Tanaka K., Kunihiro N., Kimoto K., Duong D. (eds) Mathematical Modelling for Next-Generation Cryptography, Mathematics for Industry, vol. 29, pp. 349-365, Springer, Singapore, 2016.

[11] J. Horwitz, and B. Lynn, "Towards Hierarchical Identity-Based Encryption," in Knudsen L.R. (eds.) Adavances in Cryptology - EUROCRYPT 2002, LNCS, vol. 2332, pp. 466-481, Springer, Berlin, Heidelberg, 2002.

[12] C. Gentry, and A. Silverberg, "Hierarchical ID-Based Cryptgraphy," in Zheng Y. (eds) Advances in Cryptology - ASIACRYPT 2002, LNCS, vol. 2501. , pp. 548-566, Springer, Berlin, Heidelberg, 2002.

[13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," in Cramer R. (eds) Advances in Cryptology - EUROCRYPT 2005, LNCS, vol. 3494, pp. 440-456, Springer, Berlin, Heidelberg, 2005.

[14] A. Weil, "Sur Les Fonctions Algébriques à Corps de Constantes Fini," in Comptes Rendus

Hebdomadaires des Séances de l'Academie des Sciences, vol. 210(17), pp. 589-616, 1940.

[15] J. Tate, "WC-Groups Over p-Adic Fields," in Séminaire Bourbaki: Années 1956/57-1957/58, exposés 137-168, Séminaire Bourbaki, vol. 4(156), pp. 265-277, 1958.

[16] S. Lichtenbaum, "Duality Theorems For Curves over p-adic Fields," in: Invent Math, vol. 7, pp. 120-136, Springer, 1969.

[17] V. Miller, "Short Programs of Function on Curve," unpublished manuscript, 1986.

[18] V. Miller, "The Weil Pairing, and Its Effcient Calculation," in Journal of Cryptology, vol. 17, pp. 235-261, 2004.

[19] A. Menezes, T. Okamoto, and S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field," in IEEE Trans. on Information Theory, vol. 39(5), pp. 1639-1646, 1993.

[20] A. Joux, "A One Round Protocol for Tripartite Diffe-Hellman," in Bosma W. (eds.) Algorithmic Number Theory - ANTS 2000, LNCS, vol. 1838, pp. 385-393, Springer, Berlin, Heidelberg, 2000.

[21] J. Hoffstein, J. Pipher, and J.H. Silverman, "An Intoduction to Mathematical Cryptography," Springer, New York, NY, 2008.

[22] D. Boneh, "The Decision Diffie-Hellman problem," in: Buhler J.P. (eds) Algorithmic Number Theory, ANTS 1998. LNCS, vol. 1423, pp. 48-63, Springer, Berlin, Heidelberg, 1998.

[23] L. Chen, Z. Cheng, J. Malone-Lee, and N.P. Smart, "An Effcient ID-KEM Based on the Sakai-Kasahara Key Construction," in IEEE Proceedings Information Theory, vol. 153(1), pp. 19-26, 2006.

[24] L. Martin, "Intrduction to Identity-Based Encryption (Information Security andPrivacy Series)," Artech House, Norwood, MA, USA, 2008.

[25] V. Shoup, "A Computational Introduction to Number Theory and Algebra," Cambridge University Press, New York, US, 2005.

[26] U.M. Maurer, and Y. Yacobi Y, "Non-interactive Public-Key Cryptography," in Davies D.W. (eds) Advances in Cryptology - EUROCRYPT '91, LNCS, vol. 547, pp. 498-507, Springer, Berlin, Heidelberg, 1991.

[27] O. Regev, "On Lattices, Learning With Errors, Random Linear Codes, and Cryptography," in Proceedings of The 37th Annual ACM Symposium on Theory of Computing (STOC '05), ACM, New York, NY, USA, pp. 84-93, 2005.

[28] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors For Hard Lattices and New Cryptographic Constructions," in Proceedings of the 40th annual ACM Symposium on Theory of Computing (STOC '08), ACM, New York, NY, USA, pp. 197-206, 2008.

[29] S. Yamada, "Adaptively Secure Identity-Based Encryption from Lattices with Asymptotically Shorter Public Parameters," in Fischlin M., Coron JS. (eds) Advances in Cryptology - EUROCRYPT 2016, LNCS, vol. 9666, pp. 32-62, Springer, Berlin, Heidelberg, 2016.

[30] D. Boneh, and X. Boyen, "Effcient Selective-ID Secure Identity-Based Encryption Without Random Oracles," in Cachin C., Camenisch J.L. (eds.) Advances in Cryptology - EUROCRYPT 2004, LNCS, vol. 3027, pp. 223-238, Springer, Berlin, Heidelberg, 2004.

[31] D. Moody, R. Peralta, R. Perlner, A. Regenscheid, A. Roginsky, and L. Chen, "Report on Pairing-based Cryptography," in Journal of research of the National Institute of Standards and Technology, vol. 120, pp. 11–27, 2015.

[32] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert, "Bonsai Trees, or How To Delegate a Lattice Basis," in Gilbert H. (eds) Advances in Cryptology - EUROCRYPT 2010. LNCS, vol. 6110, pp. 523-552, Springer, Berlin, Heidelberg, 2010.

[33] L. Ducas, V. Lyubashevsky, and T. Prest, "Efficient Identity-Based Encryption over NTRU Lattices," in Sarkar P., Iwata T. (eds) Advances in Cryptology - ASIACRYPT 2014, LNCS, vol. 8874, pp. 22-41, Springer, Berlin, Heidelberg, 2014.

[34] S.Y. Yan, "Quantum Computational Number Theory," Springer International Publishing, 2015.

[35] P. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," in SIAM J. Comput., vol. 26, pp. 1484-1509, 1997.

[36] L.K. Grover, "A Fast Quantum Mechanical Algorithm For Database Search," in Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC '96), ACM, New York, NY, USA, pp. 212-219, 1996.

[37] L.K. Grover, "From Schrödinger's Equation To The Quantum Search Algorithm," in Pramana - Journal of Physics, vol. 56, pp. 333-348, 2001.