applied sciences

MDPI

Article

Practical Inner Product Encryption with Constant Private Key †

Yi-Fan Tseng, Zi-Yuan Liu * and Raylin Tso

Department of Computer Science, National Chengchi University, Taipei 11605, Taiwan; yftseng@cs.nccu.edu.tw (Y.-F.T.); raylin@cs.nccu.edu.tw (R.T.)

* Correspondence: zyliu@cs.nccu.edu.tw; Tel.: +886-2-29393091 (ext. 62329)

† Proceedings of the 17th International Joint Conference on e-Business and Telecommunications—Volume 3: SECRYPT, INSTICC; SciTePress: Setubal, Portugal, 2020; pp. 553–558, doi:10.5220/0009804605530558.

Received: 7 November 2020; Accepted: 1 December 2020; Published: 3 December 2020

Abstract: Inner product encryption, first introduced by Katz et al., is a type of predicate encryption in which a ciphertext and a private key correspond to an attribute vector and a predicate vector, respectively. Only if the attribute and predicate vectors satisfy the inner product predicate will the decryption in this scheme be correct. In addition, the ability to use inner product encryption as an underlying building block to construct other useful cryptographic primitives has been demonstrated in the context of anonymous identity-based encryption and hidden vector encryption. However, the computing cost and communication cost of performing inner product encryption are very high at present. To resolve this problem, we introduce an efficient inner product encryption approach in this work. Specifically, the size of the private key is only one $\mathbb{G}$ element and one $\mathbb{Z}_p$ element, and decryption requires only one pairing computation. The formal security proof and implementation result are also demonstrated. Compared with other state-of-the-art schemes, our scheme is the most efficient in terms of the number of pairing computations for decryption and the private key length.

Keywords: predicate encryption; inner product encryption; constant-size private key; efficient decryption; constant pairing computations

1. Introduction

Inner product encryption (IPE), first introduced by Katz et al. [1], is a type of predicate encryption [2] in which a ciphertext and a private key correspond to an attribute vector $\mathbf{x}$ and a predicate vector $\mathbf{y}$, respectively. In particular, the decryption will be correct if and only if the attribute vector and the predicate vector satisfy the inner product predicate, meaning that the inner product operation of $\mathbf{x}$ and $\mathbf{y}$ equals zero ($\langle \mathbf{x}, \mathbf{y} \rangle = 0$). Over the past decade, many IPE schemes have been proposed, such as those based on pairing [3–7] and lattice [8–11]. The security definition of an IPE scheme [1] can be naturally extended from the IND–CPA security of identity-based encryption [12–14]. More precisely, under the security approach of IPE, an adversary learns nothing about the encrypted message from a ciphertext associated with an attribute vector $\mathbf{x}$ if they do not own the private key associated with a predicate vector $\mathbf{y}$ such that $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. Such a definition is also called the IND–CPA security for IPE scheme in some papers [15] and is defined as the payload-hiding property in [1]. Alternatively, the security definition defined in [1], called the attribute-hiding property, states that a ciphertext reveals nothing about the corresponding ciphertext attribute $\mathbf{x}$. However, we emphasize that the attribute-hiding property is not an absolutely necessary property for IPE. Many IPE schemes proposed in the literature achieve only IND–CPA security/payload hiding, such as that in [15–17].

In addition to their usefulness in fine-grained access control, IPE schemes can be used to construct various cryptographic primitives or can be converted to more complex primitives,

such as identity-based encryption [12–14], hidden vector encryption [2,18] and subset predicate encryption [19,20]. We refer readers to the work presented in [1,19] for details.

Although many IPE schemes have been introduced, the computing cost and communication cost of these schemes are high. In particular, the pairing operation required by existing pairing-based IPE schemes is typically linearly related to the vector length; therefore, the computational efficiency of these schemes is low. Moreover, the size of the private key of most schemes is linearly related to vector lengths. However, although the existing lattice-based IPE schemes are considered quantum-resistant, the key size of almost all schemes is too large or the message space is too small. In addition, Internet of Things devices are gradually becoming common in daily life; however, the problems mentioned in the preceding discussion make the application of an IPE scheme impractical for these resource-constrained devices. Thus, an unresolved question remains: can we obtain an efficient IPE scheme by reducing the cost of decryption and optimizing the length of the private key?

1.1. Our Contributions

Herein, we resolve the aforementioned problem by introducing an effective IPE scheme. In particular, in the proposed scheme, the length of a private key is independent of the length of the predicate vector. In addition, the decryption only requires one pairing operation; thus, the decryption is also independent of the length of the predicate vector. Rigorous proofs are provided to demonstrate that, under a modified decisional Diffie–Hellman assumption, our proposed scheme is coselective IND–CPA secure. Moreover, our proposed scheme is more efficient than other advanced schemes, as listed in Tables 1 and 3.

1.2. Related Works

1.2.1. Pairing-Based IPE Schemes

The first IPE scheme, introduced by Katz et al. [1], entails the evaluation of predicates over $\mathbb{Z}_N$ using the inner product, where N is a composite number. After this pioneering work, many studies followed. For example, Okamoto and Takashima [3] proposed the first hierarchical predicate encryption method (or delegable predicate encryption) for inner product predicates; this provides a user with functionality to delegate more restrictive functionality to another user. Attrapadung and Libert [16] constructed an IPE scheme that solves the inefficiency problem of the previous scheme. More precisely, provided that the description of the ciphertext attribute vector is not included in the ciphertext, the ciphertext overhead of the scheme is reduced to $O(1)$. By combining dual system encryption [21] and dual pairing vector spaces [3] carefully, Lewko et al. [22] obtained the first fully secure IPE scheme and hierarchical predicate encryption under the n-extended decisional Diffie–Hellman assumption. However, the security of all these previous studies was based on nonstandard assumptions. To resolve this issue, Park [23] developed the first IPE scheme under the standard assumptions (i.e., decisional bilinear Diffie–Hellman and decisional linear (DLIN) assumptions). Okamoto and Takashima [24] then introduced two nonzero inner product encryption schemes that support constant-size ciphertexts and a constant-size secret key, respectively, which are adaptively secure under the DLIN assumption in the standard model. The authors also proposed the first IPE scheme that is fully secure and fully attribute-hiding [25] as well as the first unbounded IPE scheme that is also fully secure and fully attribute-hiding in the standard model under the DLIN assumption [26]. Kawiai and Takashima [27] introduced a new notion, called IPE with ciphertext conversion, which considers the security of predicate-hiding. Zhenlin and Wei [28] then introduced another concept, called multiparty cloud computation IPE with multiplicative homomorphic property, which enables an IPE scheme to support multiparty cloud computation. Kim et al. [29] proposed a new efficient IPE scheme that only requires n exponentiation and three pairing computations for decryption. Huang et al. [30] proposed the first enabled–disabled IPE, which supports timed-release services and data self-destruction. Ramanna [15] constructed two IPE schemes using tag-based quasi-adaptive

noninteractive zero knowledge, where the first and second both have the property of constant-size ciphertext but only the second has the property of attribute-hiding. Zhang et al. [7] recently proposed a new IPE scheme based on a double encryption system; it has been demonstrated to achieve adaptive security under a weak attribute-hiding model.

As discussed subsequently, extensive research has focused on the developed and proposed schemes; however, the private key length of most schemes is linearly dependent on the vector length or requires many pairing operations, making these schemes impractical. Thus, determining how to construct a more practical scheme remains a critical area of research.

1.2.2. Lattice-Based IPE Schemes

To fend off attack from quantum computers in the future, Agrawal et al. [8] proposed the first IPE scheme based on the lattice hard assumption (i.e., the learning with error assumption, which is believed to be able to withstand quantum attacks); to do so, they modified an identity-based encryption approach proposed by Agrawal et al. [31]. Xagawa [9], inspired by the work of Agrawal et al., proposed an improved lattice-based IPE scheme that reduced the size of public parameters and ciphertext. Li et al. [10] proposed a lattice-based IPE scheme that further reduced the size of public parameters and ciphertext. In contrast to [9], their work reduced the size by a factor of $\log n$, where n is the security parameter. Wang et al. [11] recently proposed the first compact IPE scheme that employs an IPE scheme [9], fully homomorphic encryption [32] and vector-encoding schemes [33]. Although these constructions are thought to be able to withstand quantum computer attacks, they are based on the learning with errors assumption, resulting in key lengths that are still too large to be practical.

1.3. Organization

The remainder of this paper is organized as follows. In Section 2, we start by discussing some preliminaries on bilinear maps, complexity assumptions and the definition of IPE. In Section 3, we then propose our IPE scheme and demonstrate its correctness. In Section 4, we subsequently demonstrate security proofs using a modified decisional Diffie–Hellman problem, and then in Section 5, we compare our approach with other state-of-the-art schemes and reveal the implementation results. In Section 6, we finally conclude the paper.

2. Preliminaries

Herein, we present the necessary preliminaries, such as notations, complex assumptions, and the definition of an IPE scheme.

2.1. Notations

Throughout this paper, we use $x \xleftarrow{\$} S$ to denote "choose an element x randomly and uniformly from the set S" and $x \leftarrow A$ to denote "x is the output of the algorithm A". Moreover, we use $\mathbf{a}$ to denote a vector and use $\mathbf{a}_i$ to denote the i-th entry of vector $\mathbf{a}$. The inner product of these two vectors $\mathbf{x}, \mathbf{y}$ is denoted as $\langle \mathbf{x}, \mathbf{y} \rangle$. For a prime p, we use $\mathbb{Z}_p$ to denote the set of integers modulo p. Finally, we use $\mathbb{N}$ and $\mathbb{Z}$ to denote the set of positive integers and integers, respectively.

2.2. Bilinear Maps

Let $\mathbb{G}$ and $\mathbb{G}_T$ be an additive and a multiplicative cyclic group, respectively; here, the order of $\mathbb{G}$ and $\mathbb{G}_T$ is a large prime p (i.e., $|\mathbb{G}| = |\mathbb{G}_T| = p$). Then, let P be a generator of $\mathbb{G}$. A bilinear map (pairing) $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a mapping with the following properties:

- Bilinearity: For $a, b \in \mathbb{Z}_p$, $e(aP, bP) = e(P, P)^{ab}$.
- Nondegeneracy: $\exists P \in \mathbb{G}$, such that $e(P, P) \neq 1_{\mathbb{G}_T}$.
- Computability: The mapping e is efficiently computable.

In this work, we take advantage of the generalized decisional Diffie–Hellman exponent (GDDHE) problem, based on [34]. The GDDHE problem is a generic framework within which new complexity assumptions can be created. We first give an overview of the GDDHE problem. Let

- p be a prime;
- s, n be two positive integers;
- $P, Q \in \mathbb{F}_p[X_1, \ldots, X_n]^s$ be two s-tuple of n-variate polynomials over $\mathbb{F}_p$; and
- f be an n-variate polynomial in $\mathbb{F}_p[X_1, \ldots, X_n]$.

Q, Q_T are two ordered sets with multivariate polynomials, and thus, we define $Q = (q_1, q_2, \ldots, q_s)$ and $R = (r_1, r_2, \ldots, r_s)$. As stated in [34], we require $p_1 = q_1 = 1$ to be two constant polynomials. Consider a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ with the generator P of $\mathbb{G}$ and $g_T = e(P, P) \in \mathbb{G}_T$. For a vector $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_p^n$, we define

$$Q(x_1, x_2, \ldots, x_n)P = (q_1(x_1, x_2, \ldots, x_n)P, \ldots, q_s(x_1, x_2, \ldots, x_n)P) \in \mathbb{G}^s,$$

and

$$g_T^{R(x_1,x_2,\ldots,x_n)} = (g_T^{r_1(x_1,x_2,\ldots,x_n)}, \ldots, g_T^{r_s(x_1,x_2,\ldots,x_n)}) \in \mathbb{G}_T^s.$$

By "f depends on (Q, R)" we mean that there are $s^2 + s$ constants $\{a_{i,j}\}_{i,j=1}^s$ and $\{b_k\}_{k=1}^s$ such that

$$f = \sum_{i,j=1}^{s} a_{i,j} q_i q_j + \sum_{k=1}^{s} b_k r_k.$$

We say that f is independent of (Q, R) if f does not depend on (Q, R).

Definition 1 (The (Q, R, f)-GDDHE Problem)**.** *Given* $(Q(x_1, \ldots, x_n)P, g_T^{R(x_1,\ldots,x_n)}, Z) \in \mathbb{G}^s \times \mathbb{G}_T^s \times \mathbb{G}_T$, *decide if* $Z \stackrel{?}{=} g_T^{f(x_1,\ldots,x_n)}$.

Then, for an algorithm $\mathcal{A}$, the advantage of $\mathcal{A}$ in solving the (Q, R, f)-GDDHE problem is defined as

$$Adv^{(Q,R,f)\text{-GDDHE}}(\mathcal{A}) = \left| \mathcal{A}\left(Q(x_1, \ldots, x_n)P, g_T^{R(x_1,\ldots,x_n)}, g_T^{f(x_1,\ldots,x_n)}\right) - \mathcal{A}\left(Q(x_1, \ldots, x_n)P, g_T^{R(x_1,\ldots,x_n)}, Z \stackrel{\$}{\leftarrow} \mathbb{G}_T\right) \right|.$$

Boneh et al. propose that the (Q, R, f)-GDDHE problem is difficult if f is independent of (Q, R) and demonstrate that a large class of hard problems can be fit into the framework of the GDDHE problem; for instance, the DDH problem over $\mathbb{G}_T$.

Definition 2 (The decisional Diffie–Hellman problem over $\mathbb{G}_T$ ($\text{DDH}_{\mathbb{G}_T}$ problem))**.** *Let* $g_T = e(P, P)$ *be a generator of* $\mathbb{G}_T$. *Given* $(P, g_T, A = g_T^a, B = g_T^b, C) \in \mathbb{G} \times \mathbb{G}_T^4$, *where* $a, b \stackrel{\$}{\leftarrow} \mathbb{Z}_p$, *decide whether* $C = g_T^{ab}$ *or an random element from* $\mathbb{G}_T$.

By setting $Q = (1), R = (1, a, b), f = ab$, the DDH problem over $\mathbb{G}_T$ is equivalent to the (Q, R, f)-GDDHE problem. Observe that no constants exist such that the linear combination of $1, a, b$ equals ab; therefore, f is independent of (Q, R). Given the result of Boneh et al., we conclude that no algorithm is available with which to solve the $\text{DDH}_{\mathbb{G}_T}$ problem with a nonnegligible advantage. See [34] for additional details.

Next, we present a modified version of the $\text{DDH}_{\mathbb{G}_T}$ problem, which will be used in the security proof.

Definition 3 (The modified decisional Diffie–Hellman problem over $\mathbb{G}_T$ (M-DDH$_{\mathbb{G}_T}$ problem)). *Let $g_T = e(P,P)$ be a generator of $\mathbb{G}_T$. Given $(P, A' = aP, g_T, A = g_T^a, B = g_T^b, C) \in \mathbb{G}^2 \times \mathbb{G}_T^4$, where $a, b \xleftarrow{\$} \mathbb{Z}_p$, decide whether $C = g_T^{ab}$ or a random element from $\mathbb{G}_T$.*

Theorem 1 (The modified decisional Diffie–Hellman assumption over $\mathbb{G}_T$ (M-DDH$_{\mathbb{G}_T}$ assumption)). *We say that the M-DDH$_{\mathbb{G}_T}$ assumption holds if there is no algorithm $\mathcal{D}$ for solving the M-DDH$_{\mathbb{G}_T}$ problem with a nonnegligible advantage.*

Proof. Compared with the DDH$_{\mathbb{G}_T}$ problem, the instance of the M-DDH$_{\mathbb{G}_T}$ problem contains an additional element $A' = aP$. The M-DDH$_{\mathbb{G}_T}$ problem is equivalent to the (Q, R, f)-GDDHE problem with

$$Q = (1, a), R = (1, a, b), f = ab.$$

No constants exist such that the linear combination of the monomials $(1 \cdot a), 1, a, b$ equals the polynomial ab. Therefore, considering the the results of Boneh et al., we conclude that the M-DDH$_{\mathbb{G}_T}$ problem is hard. Moreover, we define the advantage for an algorithm $\mathcal{D}$ in solving the M-DDH$_{\mathbb{G}_T}$ problem as

$$Adv^{\text{M-DDH}_{\mathbb{G}_T}}(\mathcal{D}) = \left| \Pr[\mathcal{D}(P, A', g_T, A, B, C = g_T^{ab}) = 1] - \Pr[\mathcal{D}(P, A', g_T, A, B, C \xleftarrow{\$} \mathbb{G}_T) = 1] \right|.$$

□

2.3. Definition of Inner Product Encryption

An IPE scheme consists of four algorithms: **Setup**, **KeyGen**, **Encrypt** and **Decrypt**. The details of the algorithms are as follows:

- **Setup**$(1^\lambda, 1^\ell)$. Take as inputs the security parameters $(1^\lambda, 1^\ell)$, where $\lambda, \ell \in \mathbb{N}$, and the algorithm outputs the system parameter $\mathtt{params}$ and the master secret key $\mathtt{msk}$. The descriptions of the attribute vector space $\mathfrak{A}$ and the predicate vector space $\mathfrak{P}$ are implicitly included in $\mathtt{params}$. Moreover, the inner product operation over $\mathfrak{A}$ and $\mathfrak{P}$ must be well defined.
- **Encrypt**$(\mathtt{params}, \mathbf{x}, M)$. Given the system parameter $\mathtt{params}$, an attribute vector $\mathbf{x} \in \mathfrak{A}$ and a message M, the algorithm outputs a ciphertext $\mathtt{C}_\mathbf{x}$ for the attribute vector $\mathbf{x}$.
- **KeyGen**$(\mathtt{params}, \mathtt{msk}, \mathbf{y})$. Given the system parameter $\mathtt{params}$ and a predicate vector $\mathbf{y} \in \mathfrak{P}$, the algorithm outputs the private key $\mathtt{K}_\mathbf{y}$ for the predicate vector $\mathbf{y}$.
- **Decrypt**$(\mathtt{params}, \mathtt{C}_\mathbf{x}, \mathtt{K}_\mathbf{y})$. Given the system parameter $\mathtt{params}$, a ciphertext $\mathtt{C}_\mathbf{x}$ and the private key $\mathtt{K}_\mathbf{y}$, the algorithm outputs a message M or a error symbol $\perp$.

The correctness is defined as follows. For all $\lambda, \ell \in \mathbb{N}$, let $\mathtt{C}_\mathbf{x} \leftarrow$ **Encrypt**$(\mathtt{params}, \mathbf{x} \in \mathfrak{A}, M)$ and let $\mathtt{K}_\mathbf{y} \leftarrow$ **KeyGen**$(\mathtt{params}, \mathtt{msk}, \mathbf{y} \in \mathfrak{P})$; thus, we have

$$\begin{aligned} M &\leftarrow \textbf{Decrypt}(\mathtt{params}, \mathtt{C}_\mathbf{x}, \mathtt{K}_\mathbf{y}) \quad \text{if } \langle \mathbf{x}, \mathbf{y} \rangle = 0; \\ \perp &\leftarrow \textbf{Decrypt}(\mathtt{params}, \mathtt{C}_\mathbf{x}, \mathtt{K}_\mathbf{y}) \quad \text{if } \langle \mathbf{x}, \mathbf{y} \rangle \neq 0, \end{aligned}$$

where $(\mathsf{params}, \mathsf{msk}) \leftarrow$ **Setup**$(1^\lambda, 1^\ell)$.

2.4. Security Model

Here, we first introduce IND–CPA security for IPE. The IND–CPA game of IPE for the attribute vector space $\mathfrak{A}$ and predicate vector space $\mathfrak{P}$ is defined as an interactive game between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$.

- **Setup**. The challenger $\mathcal{C}$ runs **Setup**$(1^\lambda, 1^\ell)$ and sends the system parameter $\mathtt{params}$ to the adversary $\mathcal{A}$.

- **Query Phase 1**. The challenger polynomially answers many private key queries for $\mathbf{y} \in \mathfrak{P}$ for the adversary $\mathcal{A}$ by returning $\mathtt{K}_{\mathbf{y}} \leftarrow \mathbf{KeyGen}(\mathtt{params}, \mathtt{msk}, \mathbf{y})$.
- **Challenge**. The adversary $\mathcal{A}$ submits an attribute vector $\mathbf{x}^* \in \mathfrak{A}$ such that $\langle \mathbf{x}^*, \mathbf{y} \rangle \neq 0$ for all $\mathbf{y}$ that have been queried in **Query Phase 1** and two messages M_0, M_1 with the same length to challenger $\mathcal{C}$. Then, $\mathcal{C}$ randomly chooses $\beta \in \{0, 1\}$ and returns a challenge ciphertext $\mathtt{C}_{\mathbf{x}^*} \leftarrow \mathbf{Encrypt}(\mathtt{params}, \mathbf{x}^*, M_\beta)$.
- **Query Phase 2**. This phase is the same as **Query Phase 1**, except that the adversary is not allowed to make a query with $\mathbf{y} \in \mathfrak{P}$ such that $\langle \mathbf{x}^*, \mathbf{y} \rangle \neq 0$.
- **Guess**. The adversary $\mathcal{A}$ outputs a bit β' and wins the game if $\beta' = \beta$.

The advantage of an adversary for winning the IND–CPA game is defined as

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

Definition 4 (IND–CPA Security for IPE)**.** *We say that an IPE is IND–CPA secure if there is no probabilistic polynomial-time adversary $\mathcal{A}$ who wins the IND–CPA game with a nonnegligible advantage.*

As we mentioned in Section 1, in some literature [1,23], the security notions for an IPE are defined with the notions "payload hiding" and "attribute hiding". Informally, payload-hiding (or attribute-hiding) is defined to argue that a ciphertext leaks no information about the encrypted message (or attribute vector). The IND–CPA security shown in this section is equivalent to payload-hiding. We emphasize that attribute-hiding is unnecessary for an IPE scheme; in [15–17], schemes have been proposed satisfying only payload hiding.

We next present the selective security and the coselective security [16,35] for IPE. The selective IND-CPA (sIND-CPA) game is defined the same as the IND-CPA game, except that the adversary $\mathcal{A}$ is forced to commit before the **Setup** phase to an attribute vector $\mathbf{x}^*$, and $\mathcal{A}$ is not allowed to make private key queries with $\mathbf{y}$ such that $\langle \mathbf{x}^*, \mathbf{y} \rangle \neq 0$ in both **Query Phase 1** and **Query Phase 2**.

Definition 5 (sIND-CPA Security for IPE)**.** *An IPE scheme is said to be sIND–CPA secure if no probabilistic polynomial-time adversary wins the sIND–CPA game with a nonnegligible advantage.*

The coselective IND–CPA (csIND–CPA) game is defined as equal to the IND–CPA game, except that the adversary $\mathcal{A}$ is forced to commit before the **Setup** phase q to predicate vectors $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(q)}$ for the private key queries, where q is a polynomial in the security parameter λ and $\mathcal{A}$ is required to invoke the **Challenge** phase with an attribute vector $\mathbf{x}^*$ such that $\langle \mathbf{x}^*, \mathbf{y}^{(j)} \rangle \neq 0$ for $j = 1, \ldots, q$.

Definition 6 (csIND–CPA Security for IPE)**.** *An IPE scheme is said to be csIND–CPA secure if no probabilistic polynomial-time adversary wins the csIND–CPA game with a nonnegligible advantage.*

Coselective security can be understood as a complementary notion to selective security. In the selective security game, the adversary can learn the private key in accordance with its previous choices, whereas in the coselective security game, the adversary can choose its target after seeing the public parameter and learning the private keys of its choice. Although selective security and coselective security are weaker than full security, both notions are, by definition, incomparable in general by definition.

3. Proposed Inner Product Encryption Scheme

Our IPE scheme consists of four algorithms: **Setup**, **KeyGen**, **Encrypt** and **Decrypt**. The details of the proposed scheme are explained in the following.

- **Setup**$(1^\lambda, 1^\ell)$. Given the security parameters $(1^\lambda, 1^\ell)$, where $\lambda, \ell \in \mathbb{N}$, the algorithm performs as follows.
  1. Choose bilinear groups $\mathbb{G}, \mathbb{G}_T$ of prime order $p > 2^\lambda$. Let P and $g_T = e(P, P)$ be the generator of $\mathbb{G}$ and $\mathbb{G}_T$, respectively.
  2. Set the predicate vector space and the attribute vector space to $\mathbb{Z}_p^\ell$.
  3. Choose $\mathbf{s} = (s_1, s_2, \ldots, s_\ell) \xleftarrow{\$} \mathbb{Z}_p^\ell$.
  4. Compute $\widehat{\mathbf{h}} = (g_T^{s_i})_{i=1}^\ell = (\widehat{h}_1, \ldots, \widehat{h}_\ell)$.
  5. Output the system parameter $\mathtt{params} = (P, g_T, \widehat{\mathbf{h}})$, and the master secret key $\mathtt{msk} = \mathbf{s}$.
- **Encrypt**$(\mathtt{params}, \mathbf{x}, M)$. Given the system parameter $\mathtt{params}$, a vector $\mathbf{x} = (x_1, x_2, \ldots, x_\ell) \in \mathbb{Z}_p^\ell$, and a message $M \in \mathbb{G}_T$, the algorithm performs as follows.
  1. Choose $r, \delta \xleftarrow{\$} \mathbb{Z}_p$.
  2. Compute $\mathtt{C}_0 = rP$, and $\widehat{\mathtt{C}}_0 = g_T^r$.
  3. Compute $\mathtt{C}_i = \widehat{h}_i^r \cdot g_T^{\delta x_i} \cdot M$ for $i = 1$ to ℓ.
  4. Output the ciphertext $\mathtt{C}_\mathbf{x} = (\mathtt{C}_0, \widehat{\mathtt{C}}_0, \mathtt{C}_1, \mathtt{C}_2, \ldots, \mathtt{C}_\ell)$.
- **KeyGen**$(\mathtt{params}, \mathtt{msk}, \mathbf{y})$. Given the system parameter $\mathtt{params}$, a master secret key $\mathtt{msk}$, and a vector $\mathbf{y} = (y_1, y_2, \ldots, y_\ell) \in \mathbb{Z}_p^\ell$, where $\sum_{i=1}^\ell y_i \neq 0$, the algorithm performs as follows.
  1. Choose $k \xleftarrow{\$} \mathbb{Z}_p$.
  2. Compute $\mathtt{K}_0 = kP$, and $\mathtt{K}_1 = \langle \mathbf{s}, \mathbf{y} \rangle + k \mod p$.
  3. Output the private key $\mathtt{K}_\mathbf{y} = (\mathtt{K}_0, \mathtt{K}_1)$.
- **Decrypt**$(\mathtt{params}, \mathtt{C}_\mathbf{x}, \mathtt{K}_\mathbf{y})$. Given the system parameter $\mathtt{params}$, a ciphertext $\mathtt{C}_\mathbf{x}$, and the private key $\mathtt{K}_\mathbf{y}$, where $\mathbf{y} = (y_1, y_2, \ldots, y_\ell)$ the algorithm performs as follows.
  1. Compute $\mathtt{D}_0 = e(\mathtt{K}_0, \mathtt{C}_0)$.
  2. Compute $\mathtt{D}_1 = \prod_{i=1}^\ell \mathtt{C}_i^{y_i}$.
  3. Compute $\mathtt{D} = \dfrac{\mathtt{D}_0 \cdot \mathtt{D}_1}{\widehat{\mathtt{C}}_0^{\mathtt{K}_1}}$.
  4. Compute $d = (\sum_{i=1}^\ell y_i)^{-1} \mod p$.
  5. Compute $M = \mathtt{D}^d$.

Correctness

The correctness of the proposed scheme is shown as follows.

- $D_0 = e(\mathtt{K}_0, \mathtt{C}_0) = e(kP, rP) = g_T^{kr}$.
- $D_1 = \prod_{i=1}^\ell \mathtt{C}_i^{y_i} = \prod_{i=1}^\ell (\widehat{h}_i^r \cdot g_T^{\delta x_i} \cdot M)^{y_i} = \prod_{i=1}^\ell (\widehat{h}_i^{y_i})^r \cdot (g_T^{\delta x_i y_i}) \cdot (M^{y_i}) = \prod_{i=1}^\ell ((g_T^{s_i})^{y_i})^r \prod_{i=1}^\ell (g_T^{\delta x_i y_i}) \prod_{i=1}^\ell (M^{y_i}) = g_T^{r\langle \mathbf{s}, \mathbf{y} \rangle} \cdot g_T^{\delta \langle \mathbf{x}, \mathbf{y} \rangle} \cdot M^{\sum_{i=1}^\ell y_i}$.
- $\widehat{\mathtt{C}}_0^{\mathtt{K}_1} = g_T^{r\mathtt{K}_1} = g_T^{r\langle \mathbf{s}, \mathbf{y} \rangle + rk}$.
- $D = \dfrac{D_0 \cdot D_1}{\widehat{\mathtt{C}}_0^{\mathtt{K}_1}} = \dfrac{g_T^{r\langle \mathbf{s}, \mathbf{y} \rangle} \cdot g_T^{\delta \langle \mathbf{x}, \mathbf{y} \rangle} \cdot M^{\sum_{i=1}^\ell y_i} \cdot g_T^{kr}}{g_T^{r\langle \mathbf{s}, \mathbf{y} \rangle + rk}} = g_T^{\delta \langle \mathbf{x}, \mathbf{y} \rangle} \cdot M^{\sum_{i=1}^\ell y_i}$.
- We have $D = M^{\sum_{i=1}^\ell y_i}$ iff $\langle \mathbf{x}, \mathbf{y} \rangle = 0$.
- Thus $D^d = M^{\sum_{i=1}^\ell y_i \cdot ((\sum_{i=1}^\ell y_i)^{-1} \mod p)} = M$.

4. Security Analysis of the Proposed Scheme

We now provide the security proof for the coselective security of the proposed IPE scheme. In the subsequent proof, we view a vector as a row vector.

Theorem 2. *The proposed scheme is csIND–CPA secure for q private key queries, where q is a polynomial in the security parameter λ, under the M-DDH$_{\mathbb{G}_T}$ assumption.*

Proof. Given $(P, A' = aP, g_T, A = g_T^a, B = g_T^b, C)$, we build an algorithm $\mathcal{C}$ using the adversary $\mathcal{A}$ to solve the M-DDH$_{\mathbb{G}_T}$ problem as follows.

- **Init**. The adversary $\mathcal{A}$ commits q predicate vectors $\mathbf{y}^{(1)}, \ldots, \mathbf{y}^{(q)}$.
- **Setup**. $\mathcal{C}$ first finds a vector $\mathbf{u} = (u_1, u_2, \ldots, u_\ell)$ such that

$$\begin{bmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_q \end{bmatrix} \mathbf{u}^\top = \mathbf{0}_\ell^\top,$$

  where $\mathbf{0}_\ell = \underbrace{(0, 0, \ldots, 0)}_{\ell}$. Such $\mathbf{u}$ exists when $q > \ell$. The operation is to find a vector $\mathbf{u}$ such that $\langle \mathbf{u}, \mathbf{y}_j \rangle = 0$ for $j = 1$ to q. $\mathcal{C}$ then chooses $\mathbf{v} = (v_1, v_2, \ldots, v_\ell) \xleftarrow{\$} \mathbb{Z}_p^\ell$. Next, $\mathcal{C}$ computes $\widehat{\mathbf{h}} = (B^{u_i} \cdot g_T^{v_i})_{i=1}^{\ell} = (\widehat{h}_1, \ldots, \widehat{h}_\ell)$. Finally, $\mathcal{C}$ sets $\mathtt{params} = (P, g_T, \widehat{\mathbf{h}})$ and sends $\mathtt{params}$ to $\mathcal{A}$. Note that $\mathcal{C}$ implicitly sets $\mathtt{msk} = \mathbf{s} = (s_i = u_i \cdot b + v_i)_{i=1}^{\ell}$.

- **Query Phase 1**. After receiving $\mathbf{y}^{(i)} = (y_1^{(i)}, \ldots, y_\ell^{(i)})$ from $\mathcal{A}$, where $i \in [1, 2, \ldots, q]$, $\mathcal{C}$ first chooses $k \xleftarrow{\$} \mathbb{Z}_p$ and then computes $\mathtt{K}_{\mathbf{y}^{(i)}} = (\mathtt{K}_0, \mathtt{K}_1) = (kP, \langle \mathbf{v}, \mathbf{y}^{(i)} \rangle + k \mod p)$. The correctness of the private key $\mathtt{K}_{\mathbf{y}^{(i)}}$ is demonstrated as follows.

$$\begin{aligned} & \mathtt{K}_1 \\ = \; & \langle \mathbf{s}, \mathbf{y}^{(i)} \rangle + k \mod p \\ = \; & \textstyle\sum_{j=1}^{\ell} s_j y_j^{(i)} + k \mod p \\ = \; & \textstyle\sum_{j=1}^{\ell} (u_j \cdot b + v_j) \cdot y_j^{(i)} + k \mod p \\ = \; & b \textstyle\sum_{j=1}^{\ell} u_j y_j^{(i)} + \sum_{j=1}^{\ell} v_j y_j^{(i)} + k \mod p \\ = \; & b \langle \mathbf{u}, \mathbf{y}^{(i)} \rangle + \langle \mathbf{v}, \mathbf{y}^{(i)} \rangle + k \mod p \\ = \; & \langle \mathbf{v}, \mathbf{y}^{(i)} \rangle + k \mod p. \end{aligned}$$

- **Challenge**. Upon receiving $\mathbf{x}^*$, where $\langle \mathbf{x}^*, \mathbf{y}^{(i)} \rangle \neq 0$ for $i = 1, \ldots, q$, and two equal-length messages M_0, M_1 from $\mathcal{A}$, the challenger $\mathcal{C}$ performs the following.

  1. Choose $\beta \in \{0, 1\}$.
  2. Choose $\delta \xleftarrow{\$} \mathbb{Z}_p$.
  3. Set $\mathtt{C}_0' = A'$ and $\widehat{\mathtt{C}}_0' = A$.
  4. For $i = 1$ to ℓ, compute $\mathtt{C}_i' = (C^{u_i} \cdot A^{v_i} \cdot g_T^{\delta x_i^*}) \cdot M_\beta$.
  5. Set the challenge ciphertext $\mathtt{C}^* = (\mathtt{C}_0', \widehat{\mathtt{C}}_0', \mathtt{C}_1', \mathtt{C}_2', \ldots, \mathtt{C}_\ell')$.
  6. Return $\mathtt{C}^*$ to $\mathcal{A}$.

Here, we implicitly set the randomness of the encryption procedure to a. Therefore, if $C = g_T^{ab}$, then we have $\mathtt{C}'_0 = aP, \widehat{\mathtt{C}}'_0 = g_T^a$ for $i = 1, \ldots, \ell$,

$$\begin{aligned}\mathtt{C}'_i &= (C^{u_i} \cdot A^{v_i} \cdot g_T^{\delta x_i^*}) \cdot M_\beta \\ &= (g_T^{abu_i} \cdot g_T^{av_i} \cdot g_T^{\delta x_i^*}) \cdot M_\beta \\ &= (g_T^{a(bu_i+v_i)}) \cdot (g_T^{\delta x_i^*}) \cdot M_\beta \\ &= h_i^a \cdot g_T^{\delta x_i^*} \cdot M_\beta.\end{aligned}$$

Thus, the challenge ciphertext $\mathtt{C}^*$ is a valid ciphertext.

- **Query Phase 2**. This phase is the same as **Query Phase 1**.
- **Guess**. The adversary $\mathcal{A}$ outputs a bit β'. The challenger $\mathcal{C}$ outputs 1 if $\mathcal{A}$ wins the game and outputs a random bit otherwise.

Assume that the adversary $\mathcal{A}$ wins the game with advantage ϵ:

$$\left|\Pr[\beta' = \beta] - \frac{1}{2}\right| \geq \epsilon.$$

If $C = g_T^{ab}$, then the view of the adversary is identical as that in real world. Thus, we have

$$\begin{aligned}&\Pr[\mathcal{C}(P, A', g_T, A, B, C = g_T^{ab}) = 1] \\ = \;&\Pr[\beta' = \beta] \\ \geq \;&\tfrac{1}{2} + \epsilon.\end{aligned}$$

However, if C is a random element in $\mathbb{G}_T$, then the choice of β is independent from the adversary's view and we have

$$\begin{aligned}&\Pr[\mathcal{C}(P, A', g_T, A, B, C \xleftarrow{\$} \mathbb{G}_T) = 1] \\ = \;&\Pr[\beta' = \beta] \\ = \;&\tfrac{1}{2}.\end{aligned}$$

Therefore, the advantage of $\mathcal{C}$ in solving the M-DDH$_{\mathbb{G}_T}$ problem is

$$\begin{aligned}&\Big|\Pr[\mathcal{C}(P, A', g_T, A, B, C = g_T^{ab}) = 1] \\ - \;&\Pr[\mathcal{C}(P, A', g_T, A, B, C \xleftarrow{\$} \mathbb{G}_T) = 1]\Big| \\ \geq \;&\left|(\tfrac{1}{2} + \epsilon) - \tfrac{1}{2}\right| \\ \geq \;&\epsilon.\end{aligned}$$

This means that if there is an adversary winning the game with nonadvantage ϵ, then there is an algorithm $\mathcal{C}$ solving the M-DDH$_{\mathbb{G}_T}$ problem with a probability greater than ϵ. □

5. Efficiency Analysis and Implementation Results

Herein, we compare the efficiency of the proposed IPE scheme with the schemes proposed in [1,3,5–7,15,16,22–30,36] (Because [4,17] are the complete versions of [16,24], we only compare our work with [16,24]). As shown in Table 1, we compare our scheme to others in two aspects: the size of the private key and the number of pairing operations for decryption. The type of group order is also presented because the efficiency of prime order groups is higher than that of composite order bilinear groups.

As is evident in Table 1, our proposed scheme has the shortest private key length and smallest number of pairings. Moreover, both the private key length and the number of pairings in our proposed scheme are independent of the length of the predicate and attribute vectors. The most efficient existing

scheme is [29], where the private key length is three group elements and three pairings are needed for decryption. In our scheme, the private key is only an element of $\mathbb{G}$ and an element of $\mathbb{Z}_p$, and only one pairing is necessary during decryption. Furthermore, in [5], the private key length ($2m|\mathbb{G}|$) and the number of pairings ($2m$) are independent of the lengths of the vectors, where m is the leakage-resilience parameter. However, m must be at least equal to or greater than 2. Therefore, the private key length and pairing number are still larger than those obtained with our approach (this is because their scheme degenerates to a conventional IPE scheme without leakage resilience when $m = 1$).

Table 1. Comparison of our scheme's efficiency with that of other schemes. The vector length for an IPE scheme is denoted by ℓ; the bit lengths of the representations for an element in $\mathbb{Z}_p$ and $\mathbb{G}$ are denoted by $|\mathbb{Z}_p|$ and $|\mathbb{G}|$, respectively; the leakage resilience parameter is denoted by m.

Scheme	Private Key Length	Number of Pairings for Decryption	Group Order
[1]	$(2\ell+1)\|\mathbb{G}\|$	$2\ell+1$	Composite
[3]	$(\ell+3)\|\mathbb{G}\|$	$\ell+3$	Prime
[16]-1	$(\ell+1)\|\mathbb{G}\|$	2	Prime
[16]-2	$(\ell+6)\|\mathbb{G}\|+(\ell-1)\|\mathbb{Z}_p\|$	9	Prime
[22]	$(2\ell+3)\|\mathbb{G}\|$	$2\ell+3$	Prime
[24]-1	$(4\ell+1)\|\mathbb{G}\|$	9	Prime
[24]-2	$9\|\mathbb{G}\|$	9	Prime
[24]-3	$11\|\mathbb{G}\|$	11	Prime
[23]	$(4\ell+2)\|\mathbb{G}\|$	$4\ell+2$	Prime
[25]	$(4\ell+2)\|\mathbb{G}\|$	$4\ell+2$	Prime
[26]-1	$(15\ell+5)\|\mathbb{G}\|$	$15\ell+5$	Prime
[26]-2	$(21\ell+9)\|\mathbb{G}\|$	$21\ell+9$	Prime
[27]	$6\ell\|\mathbb{G}\|$	6ℓ	Prime
[28]	$\ell\|\mathbb{G}\|$	ℓ	Composite
[29]	$3\|\mathbb{G}\|$	3	Prime
[30]	$(4\ell+2)\|\mathbb{G}\|$	$4\ell+4$	Prime
[15]-1	$(2\ell+1)\|\mathbb{G}\|+(\ell-1)\|\mathbb{Z}_p\|$	3	Prime
[15]-2	$5\|\mathbb{G}\|$	3	Prime
[5]	$2m\|\mathbb{G}\|$	$2m$	Prime
[36]	$(4\ell+5)\|\mathbb{G}\|$	$4\ell+5$	Prime
[6]-1	$5\|\mathbb{G}\|$	5	Prime
[6]-2	$7\|\mathbb{G}\|$	7	Prime
[7]	$(\ell+1)\|\mathbb{G}\|$	$\ell+1$	Composite
Ours	$1\|\mathbb{G}\|+1\|\mathbb{Z}_p\|$	1	Prime

We also implemented our scheme and the schemes of [15,17,29] to compare efficiency. We chose these three schemes for the following reasons:

- Among all the existing IPE schemes, the first scheme of [16] requires the smallest number of pairings for decryption (only two pairings required);
- Among the schemes supporting constant private key length, the schemes of [15,29] require the smallest number of pairings for decryption (only three pairings required).

The environment of the implementation is presented in Table 2, and the implementation results are shown in Table 3. We implemented these schemes by using the Charm-Crypto library [37] and Python language. For schemes constructed over symmetric paring groups (the approach in [16] and our method), we selected the pairing group SS512 in [38] (also known as type A groups), and for the schemes constructed over asymmetric pairing groups (in [15,29]), we chose the pairing group BN254 in [39] (also known as type F groups). The SS512 group is a supersingular elliptic curve group where the size of the base field order is 512 bits and the embedding degree is two. For a bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ over the SS512 group, the bit lengths of elements in $\mathbb{G}$ and $\mathbb{G}_T$ are 64 and

128 bytes, respectively. In the case of the BN254 group, the size of the base field order is 256 bits and the embedding degree is 12. For a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ over the BN254 group, the bit lengths of elements in $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are 64, 128, and 384 bytes, respectively. For the length of predicate and attribute vectors, we chose $\ell = 100$. As evident in Table 3, the encryption and decryption algorithms of our scheme were highly efficient. For decryption and encryption, only 10 and 20 ms was required, respectively. Our encryption algorithm was 5, 8.5, and 13 times faster than that in [15,16,29], respectively, and our decryption algorithm was 10, 14, and 14 times faster than that in [15,16,29], respectively. Moreover, our private key length was 86, 2.6, and 4.3 times shorter than that in [15,16,29], respectively. However, as a trade-off, the length of the ciphertext in our scheme was the largest among these schemes.

Table 2. Environment of the implementation.

	Specification
OS	Ubuntu 18.04 LTS
CPU	Intel i7-4790 3.6 GHz
RAM	8 gb
Language	Python 3.6
Library	Charm-Crypto v0.50

Table 3. Implementation results.

Scheme	**Encryption Time (ms)**	**Decryption Time (ms)**	**Private Key Length (kb)**	**Ciphertext Length (kb)**
[16]	100	100	31.7	0.937
[29]	170	140	0.955	17.5
[15]	260	140	1.59	25.9
Ours	20	10	0.37	31.3

6. Conclusions

In this work, an efficient IPE scheme in which the size of the private keys and the number of pairings for decryption are constant is introduced; moreover, this scheme is coselective IND–CPA secure under the modified decisional Diffie–Hellman assumption. Comparison and experimental results are also provided to illustrate that the size and computing cost of this scheme are small. In future works, we aim to improve the efficiency by reducing the ciphertext length and provide a security proof for stronger security concerns under standard assumptions. Because the proposed scheme is based on bilinear pairing, it cannot resist quantum attacks, unlike lattice-based IPE schemes. In future work, we will explore how to construct an efficient and practical quantum-resistant IPE scheme.

Author Contributions: Conceptualization, Y.-F.T. and Z.-Y.L.; Methodology, Y.-F.T. and Z.-Y.L.; Investigation, Z.-Y.L.; Writing—Original Draft Preparation, Z.-Y.L.; Writing—Review and Editing, Y.-F.T. and R.T.; Supervision, R.T.; Project Administration, R.T.; Funding Acquisition, Y.-F.T. and R.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the Ministry of Science and Technology, Taiwan (ROC), under Project Numbers MOST 108-2218-E-004-001-, MOST 108-2218-E-004-002-MY2, MOST 109-2218-E-011-007-, and by Taiwan Information Security Center at National Sun Yat-sen University (TWISC@NSYSU).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Katz, J.; Sahai, A.; Waters, B. Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products. In *Advances in Cryptology—EUROCRYPT 2008, LNCS*; Smart, N., Ed.; Springer: Berlin/Heidelberg, Germany, 2008; Volume 4965, pp. 146–162. [CrossRef]
2. Boneh, D.; Waters, B. Conjunctive, Subset, and Range Queries on Encrypted Data. In *Theory of Cryptography, LNCS*; Vadhan, S.P., Ed.; Springer: Berlin/Heidelberg, Germany, 2007; Volume 4392, pp. 535–554. [CrossRef]
3. Okamoto, T.; Takashima, K. Hierarchical Predicate Encryption for Inner-Products. In *Advances in Cryptology—ASIACRYPT 2009, LNCS*; Matsui, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5192, pp. 214–231. [CrossRef]
4. Okamoto, T.; Takashima, K. Achieving Short Ciphertexts or Short Secret-keys for Adaptively Secure General Inner-product Encryption. *Des. Codes Cryptogr.* **2015**, *77*, 725–771. [CrossRef]
5. Kurosawa, K.; Phong, L.T. Anonymous and Leakage Resilient IBE and IPE. *Des. Codes Cryptogr.* **2017**, *85*, 273–298. [CrossRef]
6. Chen, J.; Gong, J.; Wee, H. Improved Inner-Product Encryption with Adaptive Security and Full Attribute-Hiding. In *Advances in Cryptology—ASIACRYPT 2018, LNCS*; Peyrin, T., Galbraith, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2018; Volume 1127, pp. 673–702. [CrossRef]
7. Zhang, Y.; Li, Y.; Wang, Y. Efficient Inner Product Encryption for Mobile Client with Constrained Capacity. *Int. J. Innov. Comput. I* **2019**, *15*, 209–226. [CrossRef]
8. Agrawal, S.; Freeman, D.M.; Vaikuntanathan, V. Functional Encryption for Inner Product Predicates from Learning with Errors. In *Advances in Cryptology—ASIACRYPT 2011, LNCS*; Lee, D.H., Wang, X., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 7073, pp. 21–40. [CrossRef]
9. Xagawa, K. Improved (Hierarchical) Inner-Product Encryption from Lattices. In *Public-Key Cryptography—PKC 2013, LNCS*; Kurosawa, K., Hanaoka, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 7778, pp. 235–252. [CrossRef]
10. Li, J.; Zhang, D.; Lu, X.; Wang, K. Compact (Targeted Homomorphic) Inner Product Encryption from LWE. In *Information and Communications Security, LNCS*; Qing, S., Mitchell, C., Chen, L., Liu, D., Eds.; Springer: Cham, Switzerland, 2017; Volume 10631, pp. 132–140. [CrossRef]
11. Wang, Z.; Fan, X.; Wang, M. Compact Inner Product Encryption from LWE. In *Information and Communications Security, LNCS*; Qing, S., Mitchell, C., Chen, L., Liu, D., Eds.; Springer: Cham, Switzerland, 2018; Volume 10631, pp. 141–153. [CrossRef]
12. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Advances in Cryptology—CRYPTO 1984, LNCS*; Springer: Berlin/Heidelberg, Germany, 1985; Volume 196, pp. 47–53. [CrossRef]
13. Boneh, D.; Franklin, M. Identity-Based Encryption from the Weil Pairing. In *Advances in Cryptology—CRYPTO 2001, LNCS*; Kilian, J., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2139, pp. 213–229. [CrossRef]
14. Boneh, D.; Boyen, X. Efficient Selective-ID Secure Identity Based Encryption without Random Oracles. In *Advances in Cryptology—EUROCRYPT 2004, LNCS*; Cachin, C., Camenisch, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3027, pp. 223–238. [CrossRef]
15. Ramanna, S.C. More Efficient Constructions for Inner-Product Encryption. In *Applied Cryptography and Network Security, LNCS*; Manulis, M., Sadeghi, A.R., Schneider, S., Eds., Springer: Cham, Switzerland, 2016; Volume 9696, pp. 231–248. [CrossRef]
16. Attrapadung, N.; Libert, B. Functional Encryption for Inner Product: Achieving Constant-Size Ciphertexts with Adaptive Security or Support for Negation. In *Public Key Cryptography—PKC 2010, LNCS*; Nguyen, P.Q., Pointcheval, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6056, pp. 384–402. [CrossRef]
17. Attrapadung, N.; Libert, B. Functional Encryption for Public-attribute Inner Products: Achieving Constant-size Ciphertexts with Adaptive Security or Support for Negation. *J. Math. Cryptol.* **2012**, *5*, 115–158. [CrossRef]
18. Lee, K. Efficient Hidden Vector Encryptions and Its Applications. *arXiv* **2017**, arXiv:1702.07456.
19. Katz, J.; Maffei, M.; Malavolta, G.; Schröder, D. Subset Predicate Encryption and Its Applications. In *Cryptology and Network Security, LNCS*; Capkun, S., Chow, S.S.M., Eds.; Springer: Cham, Switzerland, 2018; Volume 11261, pp. 115–134. [CrossRef]

20. Chatterjee, S.; Mukherjee, S. Large Universe Subset Predicate Encryption based on Static Assumption (without Random Oracle). In *Topics in Cryptology—CT-RSA 2019, LNCS*; Matsui, M., Ed.; Springer: Cham, Switzerland, 2019; Volume 11405, pp. 62–82. [CrossRef]
21. Waters, B. Dual System Encryption: Realizing Fully Secure IBE and HIBE under Simple Assumptions. In *Advances in Cryptology—CRYPTO 2009, LNCS*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5677, pp. 619–636. [CrossRef]
22. Lewko, A.; Okamoto, T.; Sahai, A.; Takashima, K.; Waters, B. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. In *Advances in Cryptology—EUROCRYPT 2010, LNCS*; Gilbert, H., Ed.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6110, pp. 62–91. [CrossRef]
23. Park, J.H. Inner-Product Encryption under Standard Assumptions. *Des. Codes Cryptogr.* **2011**, *58*, 235–257. [CrossRef]
24. Okamoto, T.; Takashima, K. Achieving Short Ciphertexts or Short Secret-Keys for Adaptively Secure General Inner-Product Encryption. In *Cryptology and Network Security, LNCS*; Lin, D., Tsudik, G., Wang, X., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; Volume 7092, pp. 138–159. [CrossRef]
25. Okamoto, T.; Takashima, K. Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption. In *Advances in Cryptology—EUROCRYPT 2012, LNCS*; Pointcheval, D., Johansson, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7237, pp. 591–608. [CrossRef]
26. Okamoto, T.; Takashima, K. Fully Secure Unbounded Inner-Product and Attribute-Based Encryption. In *Advances in Cryptology—ASIACRYPT 2012, LNCS*; Wang, X., Sako, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7658, pp. 349–366. [CrossRef]
27. Kawai, Y.; Takashima, K. Predicate- and Attribute-Hiding Inner Product Encryption in a Public Key Setting. In *Pairing-Based Cryptography—Pairing 2013, LNCS*; Cao, Z., Zhang, F., Eds.; Springer: Cham, Switzerland, 2014; Volume 836, pp. 113–130. [CrossRef]
28. Zhenlin, T.; Wei, Z. A Predicate Encryption Scheme Supporting Multiparty Cloud Computation. In Proceedings of the 2015 International Conference on Intelligent Networking and Collaborative Systems, Taipei, Taiwan, 2–4 September 2015; pp. 252–256. [CrossRef]
29. Kim, I.; Hwang, S.O.; Park, J.H.; Park, C. An Efficient Predicate Encryption with Constant Pairing Computations and Minimum Costs. *IEEE Trans. Comput.* **2016**, *65*, 2947–2958. [CrossRef]
30. Huang, S.Y.; Fan, C.I.; Tseng, Y.F. Enabled/Disabled Predicate Encryption in Clouds. *Future Gener. Comput. Syst.* **2016**, *62*, 148–160. [CrossRef]
31. Agrawal, S.; Boneh, D.; Boyen, X. Efficient Lattice (H)IBE in the Standard Model. In *Advances in Cryptology—EUROCRYPT 2010, LNCS*; Gilbert, H., Ed.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6110, pp. 553–572. [CrossRef]
32. Gentry, C.; Sahai, A.; Waters, B. Homomorphic Encryption from Learning with Errors: Conceptually-simpler, Asymptotically-faster, Attribute-based. In *Advances in Cryptology—CRYPTO 2013, LNCS*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8042, pp. 75–92. [CrossRef]
33. Apon, D.; Fan, X.; Liu, F.H. Vector Encoding over Lattices and Its Applications. *IACR Cryptol. EPrint Arch.* **2017**, *2017*, 455. Available online: https://eprint.iacr.org/2017/455 (accessed on 14 January 2020).
34. Boneh, D.; Boyen, X.; Goh, E.J. Hierarchical Identity Based Encryption with Constant Size Ciphertext. In *Advances in Cryptology—EUROCRYPT 2005, LNCS*; Cramer, R., Ed.; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3494, pp. 440–456. [CrossRef]
35. Attrapadung, N. Dual System Encryption via Doubly Selective Security: Framework, Fully Secure Functional Encryption for Regular Languages, and More. In *Advances in Cryptology—EUROCRYPT 2014, LNCS*; Nguyen, P.Q., Oswald, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8441, pp. 557–577. [CrossRef]
36. Xiao, S.; Ge, A.; Zhang, J.; Ma, C.; Wang, X. Asymmetric Searchable Encryption from Inner Product Encryption. In *Advances on P2P, Parallel, Grid, Cloud and Internet Computing*; Xhafa, F., Barolli, L., Amato, F., Eds.; Springer: Cham, Switzerland, 2017; pp. 123–132. [CrossRef]
37. Akinyele, J.A.; Garman, C.; Miers, I.; Pagano, M.W.; Rushanan, M.; Green, M.; Rubin, A.D. Charm: A Framework for Rapidly Prototyping Cryptosystems. *J. Cryptogr. Eng.* **2013**, *3*, 111–128. [CrossRef]

38. Lee, K.; Park, J.H. Identity-Based Revocation from Subset Difference Methods under Simple Assumptions. *IEEE Access* **2019**, *7*, 60333–60347. [CrossRef]
39. Barreto, P.S.L.M.; Naehrig, M. Pairing-Friendly Elliptic Curves of Prime Order. In *Selected Areas in Cryptography, LNCS*; Preneel, B., Tavares, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; Volume 3897, pp. 319–331. [CrossRef]