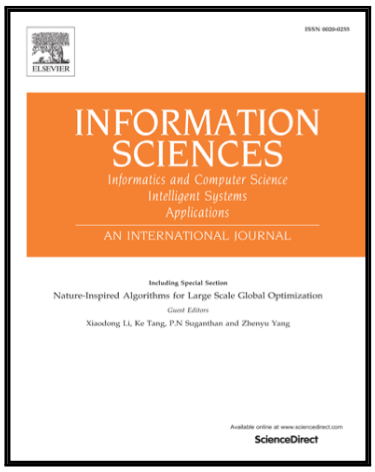
Accepted Manuscript



Efficient biometric identity-based encryption

Xiaoguo Li, Tao Xiang, Fei Chen, Shangwei Guo

PII: S0020-0255(18)30540-1
DOI: 10.1016/j.ins.2018.07.028
Reference: INS 13795

To appear in: *Information Sciences*

Received date: 9 March 2018
Revised date: 18 May 2018
Accepted date: 8 July 2018

Please cite this article as: Xiaoguo Li, Tao Xiang, Fei Chen, Shangwei Guo, Efficient biometric identity-based encryption, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.07.028

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Efficient biometric identity-based encryption

Xiaoguo Li[a], Tao Xiang[a,b,*], Fei Chen[c], Shangwei Guo[d]

[a] *College of Computer Science, Chongqing University, Chongqing 400044, China*
[b] *Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University), Ministry of Education*
[c] *Department of Computer Science and Engineering, Shenzhen University, Shenzhen 518060, China*
[d] *Department of Computer Science, Hong Kong Baptist University, Hong Kong 999077, China*

Abstract

As a special case of public key encryption, identity-based encryption (IBE) takes any public known information as public key for encryption and then decrypts a ciphertext by a well-generated private key from private key generator (PKG). Unlike the traditional IBE using a text-based identity (e-mail, etc.) as public key, in this paper, we aim to design a secure, time-saving and space-saving biometric identity-based encryption (BIBE) regarding the biometric-based identity (face, etc.) as public key. To overcome the challenge introduced by the fuzziness of biometric identities, First, we propose a provable-secure inner-product encryption (IPE) with short ciphertext and show the IPE is indistinguishable against selective identity, adaptive chosen-plaintext attack (IND-sID-CPA). Then, we construct a distance-based encryption (DBE) leveraging the proposed IPE and prove that the DBE captures the same security with the underlying IPE. Furthermore, we optimize the proposed DBE so that it also has short private key. We theoretically analyze the overhead of IPE, DBE, and optimized DBE (ODBE) in terms of time, space, and communication complexities. We also conduct experiments to measure the time and space costs of the proposed ODBE, and experimental results validate its effectiveness and efficiency.

Keywords: Biometrics, identity-based encryption, distance-based encryption, inner-product encryption, IND-sID-CPA.

1. Introduction

Identity-based encryption (IBE) possesses the ability of doing public key encryption without accessing to the public key certificate, and can be deployed in various practical applications. IBE allows for a sender to encrypt a message into a ciphertext using publicly known identity information of the receiver, such as e-mail address, social security number, or physical IP address. At the receiver's side, he can extract the message from the ciphertext by decrypting it with a key generated from the identity. Figure 1 depicts the basic principle of IBE, where Alice and Bob serve as the sender and the receiver respectively.

*Corresponding author.
Email address: txiang@cqu.edu.cn (Tao Xiang)

ACCEPTED MANUSCRIPT

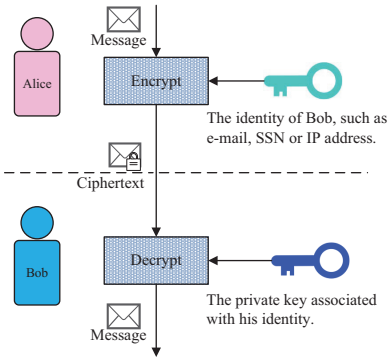


Figure 1: The principle of identity-based encryption (IBE).

One common feature of many existing IBE schemes is that they regard identity information as a string that combine the alphabet, numbers and special symbols in any order, and such identities are called *text-based identity*. The text-based solutions suffer from the following weaknesses: 1) the length of the text style identity information may be too long, it is hard for decryptor to be well-remembered; 2) the identity representations may be different in various situations, the decryptor has to derive different private keys for different representations.

To remedy these drawbacks, researchers proposed to employ one's *Biometric-based identities* instead of text-based identity in IBE [22, 23], and the corresponding schemes are called biometric identity-based encryption (BIBE). Biometric-based identities, such as face, fingerprint, pupil, etc., can offer many interesting features that text-based identities do not provide. For example, 1) biometric identity is *physical*, and one does not need to remember it; 2) biometric identity is *unique*, and one can use the same identity representations in many different situations. Furthermore, both of these features can provide safety, because no other people can forge one's biometric feature. Therefore, biometric-based identity is more secure and more convenient because it frees the user from remembering the text-style identity information.

While biometric-based identity brings a lot of benefits, it is still challenging to leverage these biometric identities as the public keys, due to the fuzziness of the biometric measurements. In traditional IBE, it must be identical between the identity generating the private key for encryption and the other one for decryption. In BIBE, however, these two identities may not be equal but they possibly belong to the same user due to the fuzziness. For this reason, the traditional IBE is out of order, and we are motivated to build a BIBE scheme that works successfully as long as two identities mentioned above are close to each other. A trivial approach is to employ a fuzzy identity-based encryption (FIBE) [42] for fault-tolerance. However, the methods of FIBE do not always suitable for practical deployment. Because the similarity measurements in FIBE are also based on text-style methods, such as Hamming distance, it is not applicable for BIBE when more practical similarity measurements are employed, such as Euclid distance and Mahalanobis distance.

ACCEPTED MANUSCRIPT

For this reason, it is necessary to design a BIBE scheme for these practical similarity measurements.

As the pioneer, Guo et al. in [22, 23] have made outstanding contributions in this research direction. Based on the Mahalanobis distance, they built a BIBE scheme, called distance-based encryption (DBE). The main idea of their proposal is to transform the distance to an inner-product form, and then derive the DBE from an inner-product encryption (IPE). However, their work may suffer from the following weaknesses in terms of efficiency and security. First, from the view of time and space efficiency: 1) the scale factor [1] in their work is about 2, and higher scale factor implies higher computational complexity and space complexity; 2) their work has short private key but long ciphertext, which is not applicable for the network-limited situation. Second, from the view of security, they did not give a proof that DBE captures the same security as the underlying IPE. For tackling these weaknesses, we are motivated to design a secure and efficient biometric identity-based encryption scheme with lower scale factor and short ciphertext, and make it suitable for the network-limited situation.

In this paper, we propose a secure and efficient biometric identity-based encryption scheme by optimized distance-based encryption. Our contributions have three salient features from the technical view. Firstly, using the symmetric of covariance matrix, we give an improved vector transformation such that a n-dimension DBE can be constructed from a $(n+2)$-dimension IPE and thus the scale factor is reduced to about 1, which saves more computational resources and space resources. Secondly, we improve the definition of DBE reasonably and appropriately. In their original definition, the threshold parameter is blurry, because the encryptor set a larger threshold may increase the probability of attacking the ciphertext. We define this parameter in the setup phase, and the sizes of private key and ciphertext are independent with threshold parameter. Thirdly, our new IPE construction aggregates all components in identity vector of the encryptor into one group element in $\mathbb{G}$, which results in short ciphertext and long private key. In [23], they aggregate all components in identity vector of the decryptor into private key, which results in short private key but long ciphertext. Therefore, our construction is suitable for network-limited situation, while the work in [23] is suitable for device-limited situation.

Our contributions can be summarized in a compact form as follows:

- We formulate the communication model of biometric identity-based encryption, and give a vector transform method, which denotes the n-dimension Mahalanobis distance by a $(n+2)$-dimension inner product.
- We propose an inner product encryption (IPE) scheme with short ciphertext. Using the proposed IPE and vector transformation, we present a provable-secure distance-based encryption (DBE) with short

[1] Scale Factor: If a distance of two d_1-dimension vectors can be represented by the inner-product of two d_2-dimension vectors, then the scale factor η is defined as $\eta = \frac{d_2}{d_1}$.

ACCEPTED MANUSCRIPT

ciphertext. We further optimize the private key of the DBE and construct an optimized distance-based encryption (ODBE) with both short ciphertext and private key.

- We show that our proposed IPE is indistinguishable against selective identity, chosen-plaintext attack (IND-sID-CPA), and formally prove that our DBE and ODBE schemes capture the same security as the IPE.
- We theoretically analyze the overhead of IPE, DBE and ODBE in terms of time, space, and communication complexities. We measure the time and space costs of ODBE by extensive experiments, and the results validate its effectiveness and efficiency.

The rest of the paper is organized as follows. Section 2 reviews the related work. Section 3 gives necessary notations and preliminaries. Section 4 presents the communication model and related definitions. Section 5 describes the construction of our IPE and DBE, and Section 6 provides their security analysis. Section 7 describes the optimized DBE and its security analysis. Section 8 provides the performance evaluation from both theoretical and experimental perspectives. Finally, Section 9 concludes the paper.

2. Related work

In 1984, Shamir [46] first introduced the notion of identity-based encryption (IBE) for eliminating the key management in a certification-based public key infrastructure (PKI). The sender encrypts messages directly with the receiver's identity (arbitrary string) and the receiver decrypts the ciphertext using a private key associated with the corresponding identity from the private key generator (PKG). Until 2001, Boneh and Franklin [10] proposed the first practical and secure IBE using bilinear map, and it is provable secure under the random oracle model [8]. Following, Waters [49] constructed an efficient IBE, which is provable secure under the standard model. Since then, IBE evolved into numerous variations, e.g. hierarchical identity-based encryption [9, 13, 24], anonymous identity-based encryption [13, 45], etc.; IBE is then also suitable to various identity related applications [15–18, 47].

In [42], Sahai and Waters first introduced the notion of fuzzy identity-based encryption (FIBE) allowing for a certain amount of error-tolerance in the identities. In an FIBE, identities are regarded as a set of descriptive attributes instead of a string of characters in standard IBE system, and a user with the private key associated with an attribute set ω is able to decrypt a ciphertext encrypted with the public key ω' if and only if the distance between ω and ω' is bounded by a predefined threshold. Since then, FIBE became an active research field and many related concepts were proposed, such as predicate encryption [29], hidden-vector encryption [12]. In recent years, the generalized concept of functional encryption (FE) [11] has been developed for providing stronger functionality. However, generic FE is still computationally expensive for

ACCEPTED MANUSCRIPT

practical usage. For improving the efficiency of FE, many FE with special functionality was proposed, such as inner-product [3, 4, 6, 30], threshold [5], garbled circuits [21], and regular languages [50].

Due to the uniqueness and the physical property, biometric features of human beings have been introduced to cryptography research community for encryption [26, 38, 43, 44, 48], digital signature [20, 27], authentication [28, 32, 34], identification [19, 51], access control [36, 37], and other security areas [14, 25, 31, 33, 35]. However, these solutions for embedding biometrics are based on the Hamming distance, and they are not applicable for many real situations those employ more practical similarity measurements, such as Euclid distance, Mahalanobis distance. In [22] and [23], a biometric identity-based encryption (BIBE) scheme based on Mahalanobis distance was proposed, which treats biometrics as public information and the private keys are generated from biometric information and a master secret key. However, their scheme has higher scale factor and long ciphertext, which is not applicable for the network-limited situation. In this paper, our goal is to design a BIBE that has lower scale factor and short ciphertext. Besides, our proposal achieves the indistinguishable against selective identity, chosen-plaintext attack (IND-sID-CPA).

3. Notations and preliminaries

We give notations, preliminaries, definitions of the key concepts used throughout the paper. Also, we present the threat model in which we analyse the security of our proposed biometric identity-based encryption.

3.1. Notations

Let $\mathbb{N}$ denote the set of natural numbers, $\mathbb{R}$ be the set of real numbers, $\mathbb{Z}_p$ be a finite field of prime order p and $[n]$ be the set $\{1, 2, \cdots, n\}$. If $n \in \mathbb{N}$, then $\{0,1\}^n$ denotes the set of n-bit strings, and $\{0,1\}^*$ is the set of all bit strings. The empty string is denoted as ε. If S is a set, then by $a \xleftarrow{R} S$ we denote that a is sampled uniformly from S. If $\mathcal{A}$ is an algorithm, then by $y \leftarrow \mathcal{A}(x)$ we denote that a deterministic algorithm $\mathcal{A}$ on input x outputs y, and by $y \xleftarrow{R} \mathcal{A}(x)$, we denote that the algorithm $\mathcal{A}$ is probabilistic. By $d(\vec{x}, \vec{y})$ and $\langle \vec{x}, \vec{y} \rangle$, we denote the Mahalanobis distance and the inner-product of two vectors $\vec{x}$ and $\vec{y}$, respectively.

3.2. Preliminaries

3.2.1. Mahalanobis distance

The Mahalanobis distance is a measure of the distance between two vectors in a multi-dimensional space. Let $\vec{x} = (x_1, \cdots, x_n)$ and $\vec{y} = (y_1, \cdots, y_n)$ be two n-dimension vectors sampled from same distribution with covariance matrix F, which is a symmetric matrix. Suppose all values are from the real number space $\mathbb{R}$. The Mahalanobis distance is defined as

$$d_M(\vec{x}, \vec{y})^2 = \sqrt{(\vec{x} - \vec{y})^T F^{-1} (\vec{x} - \vec{y})} \tag{1}$$

[2]For simplicity, we only use $d(\vec{x}, \vec{y})$ to denote the Mahalanobis distance throughout this paper.

ACCEPTED MANUSCRIPT

where $\vec{x}-\vec{y}=(x_1-y_1,\cdots,x_n-y_n)$ and F^{-1} is the inverse of F. Without loss of generality, F^{-1} is also a symmetric matrix and we define the F^{-1} as

$$F^{-1}=\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

where $a_{i,j}=a_{j,i}$ for all $1\leq i,j\leq n$ due to the symmetry of the covariance matrix F. If the covariance matrix is the identity matrix, the Mahalanobis distance reduces to the Euclidean distance. If the covariance matrix is diagonal, then the resulting distance measure is called a weighted Euclidean distance.

3.2.2. Bilinear map

Bilinear map [10] is a cryptographic tool, which has been used for a number of cryptographic constructions. Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups with the same prime order p of size κ and g be the generator of $\mathbb{G}$. A bilinear map e is a map $e:\mathbb{G}\times\mathbb{G}\mapsto\mathbb{G}_T$ with the following properties:

- *Computability*: there exists a polynomial time algorithm for computing map e efficiently;
- *Bilinearity*: for all $u,v\in\mathbb{G}$ and $a,b\in\mathbb{Z}_q$, $e(u^a,v^b)=e(u,v)^{ab}$;
- *Non-degeneracy*: there exist g_1 and g_2 such that $e(g_1,g_2)\neq 1$

The bilinear decision Diffie-Hellman exponent (BDDHE) problem in groups $(\mathbb{G},\mathbb{G}_T)$ is: given a tuple $(g,g^{\alpha^1},g^{\alpha^2},\cdots,g^{\alpha^{n-1}},g^{\alpha^{n+1}},\cdots,g^{\alpha^{2n}},h,z)$, to decide whether $z=e(g,h)^{\alpha^n}$ holds. We say that a polynomial-time adversary $\mathcal{A}$ has advantage ϵ in solving the BDDHE problem in groups $(\mathbb{G},\mathbb{G}_T)$ if

$$\left|Pr\left[\mathcal{A}(g,\cdots,g^{\alpha^{n-1}},g^{\alpha^{n+1}},\cdots,g^{\alpha^{2n}},h,z)=1\right]-Pr\left[\mathcal{A}(g,\cdots,g^{\alpha^{n-1}},g^{\alpha^{n+1}},\cdots,g^{\alpha^{2n}},h,e(g,h)^{\alpha^n})=1\right]\right|\geq\epsilon$$

where the probability is taken over the randomly chosen α,h,z and the random bits by $\mathcal{A}$.

BDDHE assumption. We say that (t,ϵ)-BDDHE assumption holds in groups $(\mathbb{G},\mathbb{G}_T)$ if no t-time adversary has the advantage at least ϵ in solving the BDDHE problem.

4. Communication model and definitions

4.1. Communication model

First, we give the communication model of biometric identity-based encryption (BIBE), which is shown in Figure 2. Our BIBE is based on distance-based encryption (DBE) that consists of four *probabilistic* or *deterministic* polynomial algorithms DBE = (Setup, KeyGen, Enc, Dec). There are three roles involved

ACCEPTED MANUSCRIPT

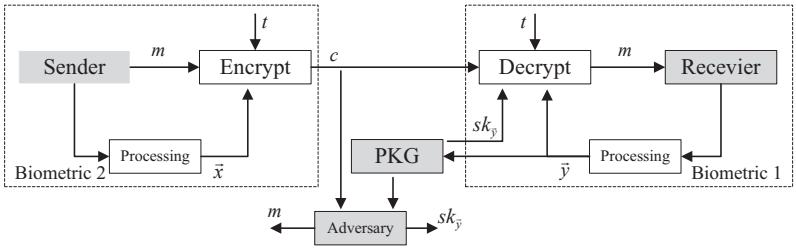


Figure 2: Communication model of biometric identity-based encryption.

in biometric identity-based cryptosystem: sender, receiver and private key generator (PKG). First, PKG invokes algorithm Setup and outputs a master public key mpk, a master secret key msk, and a threshold parameter t. Master public key and master secret key are called *public key* and *master key* for short in our subsequent statement respectively. On the receiver's side, the receiver takes a biometric trait (biometric 1) and outputs a feature vector $\vec{y}$ by an image processing procedure. Then the receiver sends $\vec{y}$ to PKG and PKG runs algorithm KeyGen to generate a private key $sk_{\vec{y}}$ for decryption. After that, the sender takes another biometric trait (biometric 2) and outputs a feature vector $\vec{x}$ by the same image processing procedure, then encrypts the message m to a ciphertext c using the algorithm Enc by taking $\vec{x}$ and a threshold t as inputs. Finally, the receiver tries to decrypt the ciphertext c using algorithm Dec by taking $sk_{\vec{y}}$ and the same threshold t as inputs.

Another role shown in Figure 2 is the adversary with the goal to recover the message m or private key $sk_{\vec{y}}$ of the receiver. In BIBE, the adversary has the ability to eavesdrop the communication between the sender and the receiver, to register a private key from PKG. For simplicity, we also assume that all the communication among the sender and the receiver are authenticated.

Compared to the model in [22], here the communication model has been improved. In the model in [22], the encryptor determines the threshold parameter. If the encryptor set a large threshold unconsciously, the probability of attacking the ciphertext by adversary may be increased. In our model, the threshold is predefined by the PKG and then anyone in the BIBE cryptosystem knows the threshold. Specifically, in the construction of our proposed DBE, the threshold serves as an input only in decryption algorithm but not encryption, this overcomes the above weakness because the sender cannot set the threshold on their own to increase the probability of being attacked by adversary.

4.2. Definitions and security model

Here we provide the related definitions and security model. Informally in the DBE, the encryption, by taking a vector $\vec{x}$ and message M as input, outputs the corresponding ciphertext CT; the decryption, by taking vector $\vec{y}$ as the private key and a threshold t, outputs the message M if and only if $d(\vec{x}, \vec{y}) \leq t$.

First, we define the DBE formally in the following:

ACCEPTED MANUSCRIPT

Definition 1. (**Distance-based encryption**)

1. $(mpk, msk, t) \xleftarrow{R}$ Setup(κ, n, F): The Setup algorithm is a probabilistic algorithm, which takes as input the security parameter κ and the distance parameter (n, F) and outputs a public key mpk, a master key msk and a threshold t.
2. $sk_{\vec{y}} \xleftarrow{R}$ KeyGen$(msk, \vec{y})$: The KeyGen algorithm is a probabilistic algorithm, which takes as input the master key msk and a n-dimension vector $\vec{y}$ and outputs a private key $sk_{\vec{y}}$.
3. $CT \xleftarrow{R}$ Enc$(mpk, \vec{x}, m)$: The Enc algorithm is a probabilistic algorithm, which takes as input the public key mpk, a n-dimension vector $\vec{x}$ and a message m, and outputs a ciphertext CT.
4. $\{m, \perp\} \leftarrow$ Dec$(mpk, sk_{\vec{y}}, t, CT)$: The Dec algorithm is a deterministic algorithm, which takes as input the public key mpk, private key $sk_{\vec{y}}$, threshold t and the ciphertext CT, and outputs the message m if and only if $d(\vec{x}, \vec{y}) \leq t$. Otherwise, it simply outputs $\perp$.

Correctness: For any pair of master key and public key $(mpk, msk) \xleftarrow{R}$ Setup(κ, n, F), any private key $sk_{\vec{y}} \xleftarrow{R}$ KeyGen$(msk, \vec{y})$, any message m and any ciphertext $CT \xleftarrow{R}$ Enc$(mpk, \vec{x}, m)$, the following condition holds:

$$\text{Dec}(mpk, sk_{\vec{y}}, t, CT) = \begin{cases} m, & \text{if } d(\vec{x}, \vec{y}) \leq t \\ \perp, & \text{if } d(\vec{x}, \vec{y}) > t \end{cases}$$

We now describe the security model of DBE, i.e. selective identity, adaptive chosen-plaintext attack (IND-sID-CPA). The security model requires that an adversary cannot distinguish which message is encrypted under well-defined security game.

First, we provide the key extraction oracle to the selective identity adversary:

- Key Extraction Oracle $\mathcal{O}_K(\vec{y})$. The adversary can issue a polynomial number of queries $\vec{y}$ to the challenger, and then the challenger responds by running algorithm KeyGen to generate a private key $sk_{\vec{y}}$ corresponding to vector $\vec{y}$. Finally, the challenger sends the private key $sk_{\vec{y}}$ to the adversary.

Then, we define the IND-sID-CPA of DBE by a game between the adversary and the challenger, which is described formally as the following five phases.

Definition 2. (**IND-sID-CPA in distance-based encryption**)

1. Setup: The challenger first runs the Setup algorithm to generate master parameters and threshold t, gives mpk and threshold t to the adversary and keeps msk by itself. At the same time, the adversary determines a vector $\vec{x}$ for the challenge in the following stage and then sends it to the challenger.
2. Query 1: The adversary can issue a polynomial number of queries to the oracles $\mathcal{O}_K(\vec{y})$. But it is required that $d(\vec{x}, \vec{y}) > t$ holds for all queried $\vec{y}$.

ACCEPTED MANUSCRIPT

3. Challenge: The adversary determines two messages m_0^* and m_1^* and sends to the challenger. Then the challenger chooses a bit $b \xleftarrow{R} \{0,1\}$, encrypts m_b^* to a ciphertext CT^* under the pre-determined identity vector $\vec{x}$ and sends it to the adversary.
4. Query 2: The adversary can issue a polynomial number of queries to the oracles $\mathcal{O}_K(\vec{y})$ as in Query 1 and it is also required that $d(\vec{x}, \vec{y}) > t$ holds for all queried $\vec{y}$.
5. Guess: The adversary outputs a guess bit b', and wins the game if $b' = b$.

The advantage of $\mathcal{A}$ is defined as $Pr[b' = b] - \frac{1}{2}$.

A DBE is (T, q_k, ϵ) IND-sID-CPA secure if for all T polynomial time adversaries who make at most q_k queries to the oracle $\mathcal{O}_K(\cdot)$, they only have a negligible advantage ϵ in the above game.

Next, we define the Inner-Product Encryption (IPE), which serves as a supportive mechanism in our DBE. An IPE scheme also includes four probabilistic or deterministic polynomial algorithms IPE = (ISetup, IKeyGen, IEnc, IDec). Unlike the definition in DBE, the receiver in IPE decrypts successfully if and only if the inner-product of two vectors equals to zero. Formally, IPE is defined as follows:

Definition 3. (**Inner-product encryption**)

1. $(impk, imsk) \xleftarrow{R}$ ISetup(κ, n): The Setup algorithm is a probabilistic algorithm, which takes as input the security parameter κ and the dimension parameter n, and outputs a public key $impk$ and a master key $imsk$.
2. $isk_{\vec{z}} \xleftarrow{R}$ IKeyGen$(imsk, \vec{z})$: The KeyGen algorithm is a probabilistic algorithm, which takes as input the master key $imsk$ and a n-dimension vector $\vec{z}$ and outputs a private key $isk_{\vec{z}}$.
3. $ICT \xleftarrow{R}$ IEnc$(impk, \vec{w}, m)$: The Enc algorithm is a probabilistic algorithm, which takes as input the public key $impk$, a n-dimension vector $\vec{w}$ and a message m, and outputs a ciphertext ICT.
4. $\{m, \perp\} \leftarrow$ IDec$(impk, isk_{\vec{z}}, ICT)$: The Dec algorithm is a deterministic algorithm, which takes as input the public key $impk$, private key $isk_{\vec{z}}$ and the ciphertext ICT, and outputs the message m if and only if $\langle \vec{w}, \vec{z} \rangle = 0$. Otherwise, it simply outputs $\perp$.

Correctness: For any pair of master key and public key $(impk, imsk) \xleftarrow{R}$ ISetup(κ, n), any private key $isk_{\vec{z}} \xleftarrow{R}$ IKeyGen$(imsk, \vec{z})$, any message m and ciphertext $ICT \xleftarrow{R}$ IEnc$(impk, \vec{w}, m)$, the following condition holds:

$$\text{IDec}(impk, isk_{\vec{z}}, ICT) = \begin{cases} m, & \text{if } \langle \vec{w}, \vec{z} \rangle = 0 \\ \perp, & \text{if } \langle \vec{w}, \vec{z} \rangle \neq 0 \end{cases}$$

We now describe the IND-sID-CPA security model of IPE. The security model requires that an adversary cannot distinguish which message is encrypted under well-defined security game.

First, we provide the key extraction oracle to the selective identity adversary:

ACCEPTED MANUSCRIPT

- Key Extraction Oracle $\mathcal{O}_{IK}(\vec{z})$. The adversary can issue a polynomial number of queries $\vec{z}$ to the challenger, and then the challenger responds by running algorithm IKeyGen to generate a private key $isk_{\vec{z}}$ corresponding to vector $\vec{z}$. Finally, the challenger sends the private key $sk_{\vec{z}}$ to the adversary.

Then, we define the IND-sID-CPA of IPE by a game between the adversary and the challenger, which is described formally as the following five phases.

Definition 4. (**IND-sID-CPA in inner-product encryption**)

1. Setup: The challenger first runs the ISetup algorithm to generate master parameters, gives $impk$ to to the adversary and keeps $imsk$ by itself. At the same time, the adversary determines a vector $\vec{w}$ for the challenge in the following stage and then sends it to the challenger.
2. Query 1: The adversary can issue a polynomial number of queries to the oracles $\mathcal{O}_{IK}(\vec{z})$. But it is required that $\langle \vec{w}, \vec{z} \rangle \neq 0$ holds for all queried $\vec{z}$.
3. Challenge: The adversary determines two messages m_0^* and m_1^* and sends them to challenger. Then the challenger chooses a bit $b \xleftarrow{R} \{0,1\}$, encrypts m_b^* to a ciphertext ICT^* under the pre-determined identity vector $\vec{w}$ and sends it to the adversary.
4. Query 2: The adversary can issue a polynomial number of queries to the oracles $\mathcal{O}_{IK}(\vec{z})$ as in Query 1 and it is also required that $\langle \vec{w}, \vec{z} \rangle \neq 0$ holds for all queried $\vec{z}$.
5. Guess: The adversary outputs a guess bit b', and wins the game if $b' = b$.

The advantage of $\mathcal{A}$ is defined as $Pr[b' = b] - \frac{1}{2}$.

A IPE is (T, q_k, ϵ) IND-sID-CPA secure if for all T polynomial time adversaries who make at most q_k queries to the oracle $\mathcal{O}_{IK}(\cdot)$, they only have a negligible advantage ϵ in the above game.

5. Constructions

In this section, we show how to construct a DBE from an IPE in a generic way. We first give a vector transformation with small scale (the scale factor in [23] is about twice of ours). Then we present an IPE with IND-sID-CPA security. Finally, we construct a DBE scheme with short ciphertext by employing the proposed IPE as the black box.

5.1. Vector transformation with small scale factor

In DBE, we consider the Mahalanobis distance $d(\vec{x}, \vec{y})$ of two vectors $\vec{x}$ and $\vec{y}$, while in IPE we are interested in the inner-product $\langle \vec{w}, \vec{z} \rangle$ of two vectors $\vec{w}$ and $\vec{z}$. Therefore, we require to find two $\vec{w}$ and $\vec{z}$ such that its inner-product $\langle \vec{w}, \vec{z} \rangle$ can be used to express the Mahalanobis distance $d(\vec{x}, \vec{y})$ in DBE. Before we describe the details for vector transformation, we first give the definition of scale factor as follows:

ACCEPTED MANUSCRIPT

Definition 5. (**Scale factor**)
If a distance of two d_1-dimension vectors can be represented by the inner-product of two d_2-dimension vectors, then the scale factor η is defined as $\eta = \frac{d_2}{d_1}$.

Now, we present the vector transformations based on the Equation (1) of Mahalanobis distance. As in [23], we also use the squared distance and the squared Mahalanobis distance can be denoted alternatively as

$$d(\vec{x}, \vec{y}) = \sum_{1 \le i,j \le n} a_{i,j}(x_i - y_i)(x_j - y_j) \tag{2}$$

Then, we have

$$\begin{aligned} d(\vec{x}, \vec{y}) &= \sum_{1 \le i,j \le n} a_{i,j}(x_i x_j - x_i y_j - x_j y_i + y_i y_j) \\ &= \sum_{1 \le i,j \le n} a_{i,j} x_i x_j + \sum_{1 \le i,j \le n} -a_{i,j}(x_i y_j + x_j y_i) \\ &\quad + \sum_{1 \le i,j \le n} a_{i,j} y_i y_j \end{aligned}$$

Now we analyze the coefficient of $x_i y_j$ from two cases. Case 1): when $i \neq j$, because $x_i y_j$ appears twice in the above equation, $-a_{i,j}(x_i y_j + x_j y_i)$ and $-a_{j,i}(x_j y_i + x_i y_j)$, then the coefficient of $x_i y_j$ is $-(a_{i,j} + a_{j,i})$. Due to the symmetric $a_{i,j} = a_{j,i}$, the coefficient of $x_i y_j$ is $-2a_{i,j}$. Case 2): when $i = j$, the coefficient of $x_i y_i$ is $-2a_{i,i}$ because $-a_{i,j}(x_i y_j + x_j y_i) = -2a_{i,j} x_i x_j$. Thus, we have

$$\begin{aligned} d(\vec{x}, \vec{y}) &= \sum_{1 \le i,j \le n} a_{i,j} x_i x_j + \sum_{1 \le i,j \le n} -2a_{i,j} x_i y_j \\ &\quad + \sum_{1 \le i,j \le n} a_{i,j} y_i y_j \end{aligned}$$

Let X, Y, $a_i(\vec{y})$ be defined as follows

$$X = \sum_{1 \le i,j \le n} a_{i,j} x_i x_j$$

$$Y = \sum_{1 \le i,j \le n} a_{i,j} y_i y_j$$

and

$$f_i(\vec{y}) = \sum_{j=1}^{n} -2a_{i,j} y_j$$

Then, we obtain that

$$\begin{aligned} d(\vec{x}, \vec{y}) &= X + \sum_{i=1}^{n} x_i \cdot f_i(\vec{y}) + Y \\ &= \langle \vec{w}, \vec{z} \rangle \end{aligned}$$

ACCEPTED MANUSCRIPT

where $\vec{w}$ and $\vec{z}$ are two $(n+2)$-dimension vectors that are defined as

$$\vec{w} = (x_1, x_2, \cdots, x_n, X, 1) \tag{3}$$

and

$$\vec{z} = (f_1(\vec{y}), f_2(\vec{y}), \cdots, f_n(\vec{y}), 1, Y) \tag{4}$$

Since that the DBE decrypts successfully when $d(\vec{x}, \vec{y}) \leq t$, but the IPE requires that $\langle \vec{w}, \vec{z} \rangle = 0$. For adapting the IPE to DBE we should relax the IPE to decrypt when $\langle \vec{w}, \vec{z} \rangle \leq t$. It means that at least one of the following holds $\langle \vec{w}, \vec{z}_\delta \rangle = 0$, where

$$\vec{z}_\delta = (f_1(\vec{y}), f_2(\vec{y}), \cdots, f_n(\vec{y}), 1, Y - \delta) \tag{5}$$

and $\delta \in [0, t]$. Then we have $\exists \delta \in [0, t]$ such that

$$\langle \vec{w}, \vec{z}_\delta \rangle = \langle \vec{w}, \vec{z} \rangle - \delta = d(\vec{x}, \vec{y}) - \delta \tag{6}$$

Thus we have $\delta = d(\vec{x}, \vec{y})$.

As $\vec{z}_\delta$, we also define the $\vec{w}_\delta$ as follows:

$$\vec{w}_\delta = (x_1, x_2, \cdots, x_n, X - \delta, 1) \tag{7}$$

Form above, we know Mahalanobis distance of two n-dimension vectors can be denoted by the inner-product of two $(n+2)$-dimension vectors and we define the scale factor as in Definition 5. Thus, the scale factor η in our work is $\eta = \frac{n+2}{n}$, while in [23] the scale factor is $\eta = \frac{2n+2}{n}$. Although, in [22], their scale factor is also $\frac{n+2}{n}$, but they leveraged a Euclidean distance in their work, which is just a special case of Mahalanobis distance.

However, for adopting the Mahalanobis distance, two aspects must be taken into consideration: 1) All the parameters $\vec{x}$, $\vec{y}$, F^{-1} in the Mahalanobis distance should be integers. If the parameters are decimal, as in [23], we can adjust all values to integers by right shifting the decimal points. 2) The distance should be an integer and we hence adopt the squared Mahalanobis distance in the construction of DBE. In this paper, for simplicity, we directly assume all values of the defined parameters and distance to be integers.

5.2. IPE with short ciphertext

In this part, we propose a new IPE with IND-sID-CPA security. For simplicity, we only present the construction of n-dimension instead of a $(n+2)$ dimension. This is because it can be extended to a $(n+2)$ dimension straightforwardly and then followed by applying to DBE directly.

We first demonstrate the principal difference of our IPE and the IPE in [23] in a high level view. Let $\vec{\alpha}$ be the system parameter, $\vec{w}$ and $\vec{z}$ be the identity vectors for encryption and decryption, respectively. The

ACCEPTED MANUSCRIPT

IPE in [23] basically uses Equation (8) to evaluate the inner-product $\langle \vec{w}, \vec{z} \rangle$, where $\langle \vec{\alpha}, \vec{z} \rangle$ is embedded into private key and $\vec{w} + \vec{\alpha}$ is embedded into ciphertext, so it results in short private key but long ciphertext. Our IPE in a high level has the form as shown in Equation (9), where $\vec{z} + \vec{\alpha}$ is embedded into private key and $\langle \vec{\alpha}, \vec{w} \rangle$ is embedded into ciphertext, therefore our IPE has short ciphertext but long private key.

$$\langle \vec{w}, \vec{z} \rangle = \langle \vec{w} + \vec{\alpha}, \vec{z} \rangle - \langle \vec{\alpha}, \vec{z} \rangle \tag{8}$$

$$\langle \vec{w}, \vec{z} \rangle = \langle \vec{z} + \vec{\alpha}, \vec{w} \rangle - \langle \vec{\alpha}, \vec{w} \rangle \tag{9}$$

Construction 1. (**Inner-product encryption**)

1. $(impk, imsk) \xleftarrow{R}$ ISetup(κ, n):
   (a) Choose group parameters $(\mathbb{G}, \mathbb{G}_T, g, p, e)$, where $\mathbb{G}$ and $\mathbb{G}_T$ are two groups with κ-bit prime order p, and g is a generator of group $\mathbb{G}$.
   (b) Choose $\gamma, \beta, \eta, \alpha_i \xleftarrow{R} \mathbb{Z}_p$ for all $i \in [n]$.
   (c) Compute $g_i = g^{\alpha_i}$ for all $i \in [n]$, $v = g^{\beta}$, and $u = e(g, g)^{\gamma}$.
   (d) Return $impk = (n, \mathbb{G}, \mathbb{G}_T, g, p, e, [g_i], v, u, g^{\eta})$ and $imsk = (g^{\gamma})$. [3]
2. $isk_{\vec{z}} \xleftarrow{R}$ IKeyGen$(imsk, \vec{z})$:
   (a) Choose $t \xleftarrow{R} \mathbb{Z}_p$.
   (b) Compute $isk_1 = g^t$, $isk_2^i = (g^{\eta z_i} g_i)^t$ for all $i \in [n]$ and $isk_3 = g^{\gamma} v^t$.
   (c) Return $isk_{\vec{z}} = (isk_1, [isk_2^i], isk_3)$.
3. $ICT \xleftarrow{R}$ IEnc$(impk, \vec{w}, m)$:
   (a) Choose $s \xleftarrow{R} \mathbb{Z}_p$ and compute $C_1 = u^s \cdot m$ and $C_2 = g^s$.
   (b) Compute $C_3 = (v \prod_{i=1}^{n} g_i^{w_i})^s$.
   (c) Return $ICT = (C_1, C_2, C_3)$.
4. $\{m, \perp\} \leftarrow$ IDec$(impk, isk_{\vec{z}}, ICT)$:
   (a) Compute $e_1 = e(isk_3 \cdot \prod_{i=1}^{n} (isk_2^i)^{w_i}, C_2)$.
   (b) Compute $e_2 = e(isk_1, C_3)$.
   (c) Return $m = C_1 \cdot e_1^{-1} \cdot e_2$.

Correctness. We show that the decryption is correct if the inner-product $\langle \vec{w}, \vec{z} \rangle = 0$. If $\langle \vec{w}, \vec{z} \rangle = 0$, then

[3] For simplicity, $[g_i]$ denotes the set $\{g_1, g_2, \cdots, g_n\}$ and we use the same manner to represent the notations, such as $[\alpha_i]$, $[C_i]$.

ACCEPTED MANUSCRIPT

we have

$$\begin{aligned}
e_{11} &= e(\prod_{i=1}^{n}(isk_2^i)^{w_i}, C_2) \\
&= e(\prod_{i=1}^{n}((g^{\eta z_i}g_i)^t)^{w_i}, g^s) \\
&= e(\prod_{i=1}^{n}(g^{\eta z_i}g^{\alpha_i})^{w_i}, g)^{st} \\
&= e(\prod_{i=1}^{n}(g^{\eta z_i})^{w_i}, g)^{st} \cdot e(\prod_{i=1}^{n}(g^{\alpha_i})^{w_i}, g)^{st} \\
&= e(g^{\langle\vec{w},\vec{z}\rangle}, g)^{\eta st} \cdot e(g^{\langle\vec{w},\vec{\alpha}\rangle}, g)^{st} \\
&= e(g,g)^{\eta st\langle\vec{w},\vec{z}\rangle} \cdot e(g,g)^{st\langle\vec{w},\vec{\alpha}\rangle} \\
e_{12} &= e(isk_3, C_2) \\
&= e(g^{\gamma}v^t, g^s) \\
&= e(g^r(g^{\beta})^t, g^s) \\
&= e(g,g)^{sr+st\beta} \\
e_2 &= e(isk_1, C_3) \\
&= e(g^t, (v\prod_{i=1}^{n}g_i^{w_i})^s) \\
&= e(g, g^{\beta}\prod_{i=1}^{n}(g^{\alpha_i})^{w_i})^{st} \\
&= e(g,g^{\beta})^{st} \cdot e(g, \prod_{i=1}^{n}(g^{\alpha_i})^{w_i})^{st} \\
&= e(g,g)^{st\beta} \cdot e(g,g)^{st\cdot\langle\vec{w},\vec{\alpha}\rangle} \\
&= e(g,g)^{st\beta+st\cdot\langle\vec{w},\vec{\alpha}\rangle}
\end{aligned}$$

Since that $e_1 = e_{11} \cdot e_{12}$, and then it is clear that $C_1 \cdot e_1^{-1} \cdot e_2 = m$. It completes the correctness proof.

5.3. DBE with short ciphertext

In this section, we construct a new DBE with short ciphertext using the proposed IPE. Suppose the IPE scheme is a tuple of four algorithms (ISetup, IKeyGen, IEnc, IDec) as constructed in Section 5.2. With the vector transformation in Section 5.1, we now present our construction of DBE as follows.

Construction 2. (**Distance-based encryption**)

1. $(mpk, msk, t) \xleftarrow{R}$ Setup(κ, n, F):
   (a) Run algorithm $(impk, imsk) \xleftarrow{R}$ ISetup(κ, n).

ACCEPTED MANUSCRIPT

(b) Choose a reasonable threshold t according to F and n.[4]

(c) Return $mpk = (impk, F, n)$, $msk = imsk$ and t.

2. $sk_{\vec{y}} \xleftarrow{R}$ KeyGen$(msk, \vec{y})$:

(a) Compute vector $\vec{z}$ from $\vec{y}$ by Equation (4).

(b) Run algorithm $isk_{\vec{z}_\delta} \xleftarrow{R}$ IKeyGen$(imsk, \vec{z}_\delta)$ for $\delta = 0, 1, 2, 3, \cdots, t$.

(c) Return $sk_{\vec{y}} = \{isk_{\vec{z}_\delta} : \delta = 0, 1, 2, 3, \cdots, t\}$.

3. $CT \xleftarrow{R}$ Enc$(mpk, \vec{x}, m)$:

(a) Compute vector $\vec{w}$ from $\vec{x}$ by Equation (3).

(b) Run algorithm $ICT \xleftarrow{R}$ IEnc$(impk, \vec{w}, m)$.

(c) Return $CT = ICT$.

4. $\{m, \perp\} \leftarrow$ Dec$(mpk, sk_{\vec{y}}, CT)$:

(a) Compute $\delta = d(\vec{x}, \vec{y})$.

(b) If $\delta \in [0, t]$, extract $isk_{\vec{z}_\delta}$ from $sk_{\vec{y}}$, and then running the decryption algorithm

$$m' = \text{IDec}(impk, isk_{\vec{z}_\delta}, ICT)$$

(c) Else output $\perp$.

Correctness. We show that the decryption is correct when the Mahalanobis distance $d(\vec{x}, \vec{y}) \leq t$. In the decryption, IDec algorithm is employed to decrypt the ciphertext. IDec can decrypt correctly, which implies that our DBE decrypts correctly. From Equation (6) we have

$$\langle \vec{w}, \vec{z}_\delta \rangle = d(\vec{x}, \vec{y}) - \delta = \delta - \delta = 0$$

Therefore we show $\langle \vec{w}, \vec{z}_\delta \rangle = 0$, which completes the proof.

6. Security analysis

In this section, we analyze the security of our DBE and show that our DBE captures the provable semantic security by security reduction, which is presented in a high level view as follows

$$\text{BDDHE} \leqslant_p \text{z-IPE} \leqslant_p \text{IPE} \leqslant_p \text{DBE} \tag{10}$$

where $\leqslant_p$ is the hardness reduction, z-IPE denotes the selectively secure zero IPE proposed in [7], which is selectively secure under the Bilinear Decision Diffie-Hellman Exponent assumption (BDDHE). We first proof that our proposed IPE captures the same security level as z-IPE achieves, then we proof that our DBE captures the same security level as our proposed IPE achieves.

[4]The method to chose a reasonable threshold is not the core work of this paper and it has been studied extensively in the pattern recognition community.

ACCEPTED MANUSCRIPT

6.1. Security analysis of IPE

In the following Theorem 1, we prove that our IPE captures the same security level as z-IPE achieves. This implies that our proposed IPE is selectively secure under the BDDHE assumption.

Theorem 1. *Let $\mathcal{A}$ be a selective (n, T, q_k, ϵ)-adversary on our n-dimension IPE with a non-negligible advantage ϵ, then there is a $(n+1, T', q'_k, \epsilon')$-adversary $\mathcal{B}$ can break $(n+1)$-dimension IPE with another non-negligible advantage ϵ', where $T' \approx T$, $q'_k = q_k$ and $\epsilon' = \epsilon$.*

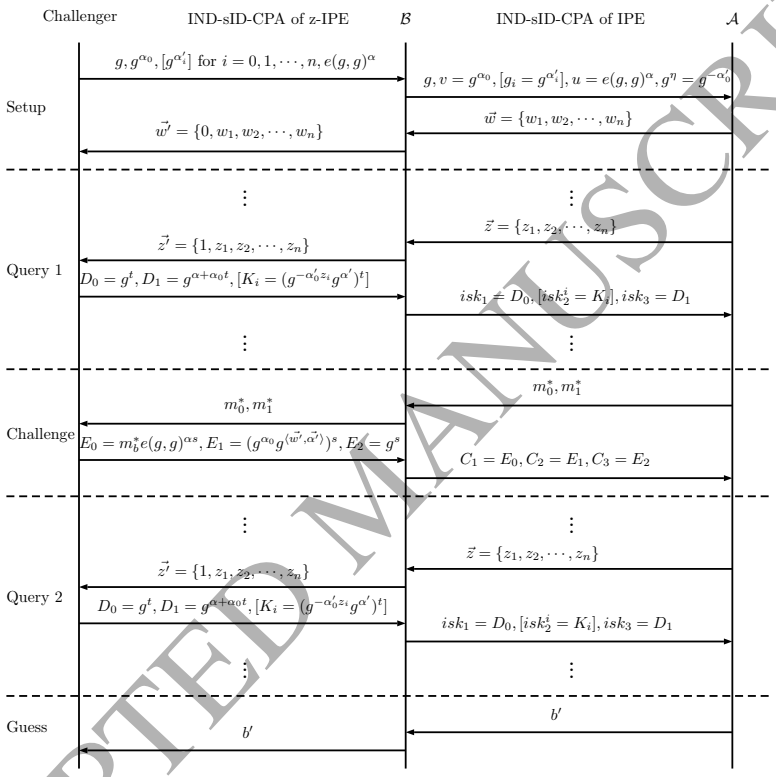


Figure 3: High-level illustration of the security proof of inner-product encryption.

Proof. Let $\mathcal{A}$ be the attacker that breaks the semantic security game of our IPE with ϵ advantage in T time after at most q_k queries to $\mathcal{O}_K$. Then we can build an adversary $\mathcal{B}$ that uses $\mathcal{A}$ as a block box and breaks the semantic security of z-IPE with advantage $\epsilon' = \epsilon$. $\mathcal{B}$'s goal is to win the semantic security game of z-IPE and $\mathcal{B}$ interacts with $\mathcal{A}$ as follows, which has also been depicted in Figure 3. Please note that $\mathcal{B}$ serves as not only the adversary in the semantic security game of z-IPE, but also the simulator in the semantic security game of our proposal IPE.

1. Setup: The challenger first runs the Setup algorithm of z-IPE to generate master parameters, then gives public parameter $g, g^{\alpha_0}, [g^{\alpha'_i}]$ for $i = 0, 1, \cdots, n$ and $e(g,g)^{\alpha}$ to $\mathcal{B}$ and keeps g^{α} by itself. Let

ACCEPTED MANUSCRIPT

$\vec{\alpha'} = \{\alpha'_0, \alpha'_1, \cdots, \alpha'_n\}$, then $\mathcal{B}$ sets the *impk* as follows: $g_i = g^{\alpha'_i}$ for $i = 1, \cdots, n$, $v = g^{\alpha_0}$, $u = e(g,g)^{\alpha}$, and $g^{\eta} = g^{-\alpha'_0}$, where $\alpha_i = \alpha'_i$ for $i = 1, \cdots, n$, $\beta = \alpha_0$, $\gamma = \alpha$ and $\eta = -\alpha'_0$ all are the unknown secret from public parameter of z-IPE. Let $\vec{\alpha} = \{\alpha_1, \alpha_2, \cdots, \alpha_n\}$, then $\mathcal{B}$ gives the public information to adversary $\mathcal{A}$. The adversary $\mathcal{A}$ determines a vector $\vec{w}$ and then sends it to $\mathcal{B}$. $\mathcal{B}$ sets $\vec{w'} = \{0, w_1, \cdots, w_n\}$ and gives $\vec{w'}$ to the challenger. Please note that the game in z-IPE is $n+1$ dimensions and the game in our IPE is n dimensions.

2. Query 1: The adversary $\mathcal{A}$ can issue a polynomial number of queries to the oracles $\mathcal{O}_K(\vec{z})$. It is required that $\langle \vec{w}, \vec{z} \rangle \neq 0$ holds for all queried $\vec{z}$. $\mathcal{B}$ serves as the oracle and responses the private key as follows: If the adversary submits a query $\vec{z}$ to key extraction oracle $\mathcal{O}_K(\vec{z})$, $\mathcal{B}$ first obtains the vector $\vec{z'}$ from $\vec{z}$ by setting $\vec{z'} = (1, z_1, z_2, \cdots, z_n)$ and sends $\vec{z'}$ to the challenger. Then the challenger runs key extraction algorithm of z-IPE and sends the private key of $\vec{z'}$ to $\mathcal{B}$. Let $D_0 = g^t$, $D_1 = g^{\alpha + \alpha_0 t}$ and $K_i = (g^{-\alpha'_0 z_i} g^{\alpha'_i})^t$ for $i = 1, \cdots, n$ be the private key. $\mathcal{B}$ can simulate the private key of vector $\vec{z}$ by setting $isk_1 = D_0$, $isk_2^i = K_i$ for $i = 1, \cdots, n$ and $isk_3 = D_1$. Finally, $\mathcal{B}$ sends the private key to $\mathcal{A}$. In this private key simulation, t is uniformly random in $\mathbb{Z}_p$ and the adversary cannot gain additional information beyond the private key.
3. Challenge: The adversary $\mathcal{A}$ determines two messages m_0^* and m_1^*. Then $\mathcal{A}$ sends them to $\mathcal{B}$. $\mathcal{B}$ gives m_0^*, m_1^* to the challenger. The challenger chooses a bit $b \xleftarrow{R} \{0,1\}$, encrypts m_b^* to the ciphertext C_b^*, and sends it to $\mathcal{B}$. Let $C_b^* = (E_0, E_1, E_2)$, where $E_0 = m_b^* \cdot e(g,g)^{\alpha s}$, $E_1 = (g^{\alpha_0} g^{\langle \vec{w'}, \vec{\alpha'} \rangle})^s$ and $E_2 = g^s$. Then $\mathcal{B}$ sets the ciphertext ICT_b^* as follows: $C_1 = E_0$, $C_2 = E_1 = (g^{\alpha_0} g^{\langle \vec{w'}, \vec{\alpha'} \rangle})^s = (g^{\beta} g^{\langle \vec{w}, \vec{\alpha} \rangle})^s = (v \prod_{i=1}^{n} g_i^{w_i})^s$ and $C_3 = E_2$. Finally, $\mathcal{B}$ responds $\mathcal{A}$ with ICT_b^*.
4. Query 2: The adversary can issue a polynomial number of queries to the oracle $\mathcal{O}_K(\vec{z})$ as he does in Query 1. It is also required that $\langle \vec{w}, \vec{z} \rangle \neq 0$ holds for all queried $\vec{z}$. $\mathcal{B}$ answers the queries in the same manner with what he does in Query 1.
5. Guess: The adversary $\mathcal{A}$ outputs a guess bit b' to $\mathcal{B}$ and $\mathcal{B}$ bets b'.

If $\mathcal{A}$ can break the semantic security of our proposed IPE with a non-negligible advantage ϵ, then $\mathcal{B}$ also can distinguish the ciphertexts of m_0^* and m_1^* with a non-negligible advantage $\epsilon' = \epsilon$ in the security game of z-IPE. It is clear that $q'_k = q_k$ and $T' = T$ because at each time the adversary queries the key extraction oracle in IPE, $\mathcal{B}$ has to query the corresponding key extraction oracle in z-IPE. This completes the proof. □

6.2. Security analysis of DBE

Theorem 2. *Let $\mathcal{A}$ be a (T, q_k, ϵ)-adversary that can attack our proposed DBE with a non-negligible advantage ϵ. Then there is a (T', q'_k, ϵ')-adversary that can attack our IPE with another non-negligible advantage ϵ', where $T' \approx (t+1) \cdot T$, $q'_k = (t+1) \cdot q_k$ and $\epsilon' = \epsilon$, where t is the threshold parameter in DBE.*

ACCEPTED MANUSCRIPT

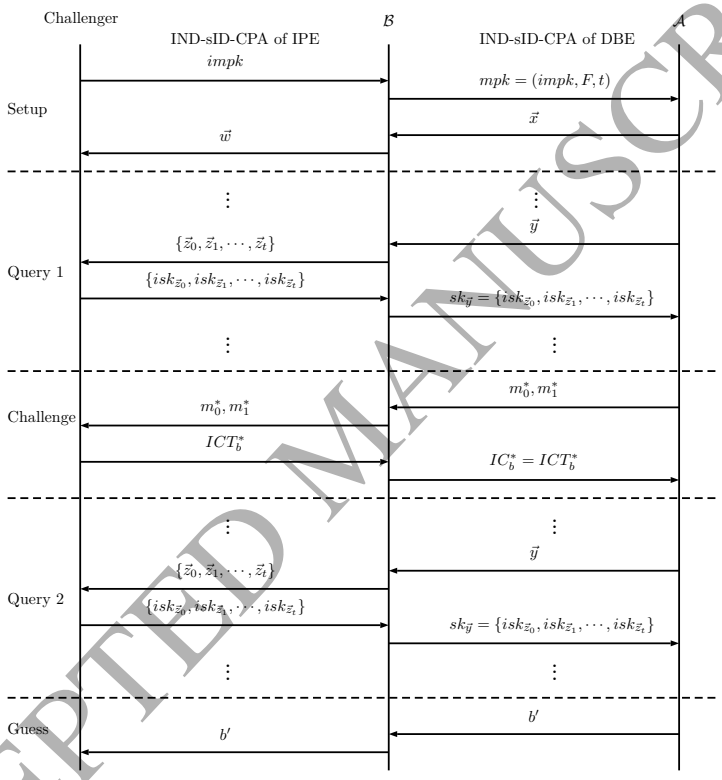


Figure 4: High-level illustration of the security proof of distance-based encryption.

ACCEPTED MANUSCRIPT

Proof. Let $\mathcal{A}$ be the attacker that breaks the IND-sID-CPA security game of distance-based encryption with ϵ advantage in T time after at most q_k queries to $\mathcal{O}_K$, at most q_d queries to $\mathcal{O}_D$. Then we build an adversary $\mathcal{B}$ that uses $\mathcal{A}$ as a block box and breaks the semantic security of our IPE with advantage $\epsilon' = \epsilon$. $\mathcal{B}$'s goal is to decide which message, m_0^* or m_1^*, is encrypted in the IND-sID-CPA security game of IPE. $\mathcal{B}$ interacts with $\mathcal{A}$ in the security game as follows, which has also been depicted in Figure 4. Please note that $\mathcal{B}$ serves as not only the adversary in the IND-sID-CPA security game of IPE, but also the challenger in the IND-sID-CPA security game of DBE.

1. Setup: The challenger first runs the ISetup algorithm to generate master parameters, gives $impk$ to $\mathcal{B}$, and keeps $imsk$ by itself. Then $\mathcal{B}$ chooses the appropriate parameters covariance matrix F and threshold t, and sends $mpk = (impk, F, t)$ to $\mathcal{A}$. After that, $\mathcal{A}$ determines a vector $\vec{x}^*$ for challenge and then sends it to $\mathcal{B}$. Finally, $\mathcal{B}$ transforms $\vec{x}$ to $\vec{w}$ by Equation (3) and sends $\vec{w}$ to the challenger.
2. Query 1: The adversary can issue a polynomial number of queries to the oracle $\mathcal{O}_K(\vec{y})$, which requires that $d(\vec{x}, \vec{y}) > t$. The oracle is defined in the following procedure: If the adversary submits a query $\vec{y}$ to key extraction oracle $\mathcal{O}_K(\vec{y})$, $\mathcal{B}$ first obtains the vector $\vec{z}_\delta$ for each $0 \leq \delta \leq t$ from $\vec{y}$ by Equation (5) and sends them to oracle $\mathcal{O}_{IK}(\vec{z})$. Then the challenger runs algorithm IKeyGen $t+1$ times and sends the private keys $[isk_{\vec{z}_\delta}]$ to $\mathcal{B}$. Finally, $\mathcal{B}$ sets $sk_{\vec{y}} = \{isk_{\vec{z}_\delta} : \delta = 0, 1, 2, 3, \cdots, t\}$ and responds $isk_{\vec{y}}$ to $\mathcal{A}$.
3. Challenge: The adversary $\mathcal{A}$ determines two messages m_0^* and m_1^*. Then $\mathcal{A}$ sends them to $\mathcal{B}$. $\mathcal{B}$ gives m_0^*, m_1^* to the challenger. The challenger chooses a bit $b \xleftarrow{R} \{0, 1\}$, encrypts m_b^* to the ciphertext ICT_b^*, and sends it to $\mathcal{B}$. Then $\mathcal{B}$ sends the ciphertext $CT_b^* = ICT_b^*$ to the adversary.
4. Query 2: The adversary can issue a polynomial number of queries to the oracle $\mathcal{O}_K(\vec{y})$ as he does in Query 1. It is also required that $d(\vec{x}, \vec{y}) > t$ holds for all queried $\vec{y}$. $\mathcal{B}$ answers the queries in the same manner with what he does in Query 1.
5. Guess: The adversary outputs a guess bit b' to $\mathcal{B}$ and $\mathcal{B}$ outputs b'.

If $\mathcal{A}$ can break the security of the DBE with a non-negligible advantage ϵ, then $\mathcal{B}$ also can distinguish the ciphertexts of m_0^* and m_1^* with a non-negligible advantage $\epsilon' = \epsilon$. Now we analyze the complexity of $\mathcal{A}$ from above interaction. Since that in the key extraction oracle of DBE, the adversary $\mathcal{B}$ queries the $\mathcal{O}_{IK}(\vec{z})$ $(t+1)$ times, so we have $q_k' = (t+1) \cdot q_k$ and $T' \approx (t+1) \cdot T$, where t is the threshold parameter. This completes the proof. □

7. Optimization on DBE with short key

In this section, we further optimize our proposed DBE. As we can see from the construction of DBE in Section 5, it has short ciphertext; however it has long private key, which causes inconvenience for the

ACCEPTED MANUSCRIPT

decryptor in practice. This is because that the decryptor has to store all the private keys of the vector $\vec{z_\delta}$ by their own, and then accesses the corresponding decrypting key in the decryption algorithm.

To reduce the size of private key, we optimize our DBE by letting the decryptor calculate decrypting key when it is necessary in the decryption algorithm. The optimized scheme is called optimized distance-based encryption (ODBE). In detail, our proposed ODBE works as follows.

1. $(mpk, msk, t) \xleftarrow{R} \text{Setup}(\kappa, n, F)$:
   (a) Run algorithm $(impk, imsk) \xleftarrow{R} \text{ISetup}(\kappa, n)$.
   (b) Choose a reasonable threshold t according to F and n.
   (c) Return $mpk = (impk, F, n)$, $msk = imsk$ and t.
2. $isk_{\vec{z}_\delta} \xleftarrow{R} \text{KeyGen}(msk, \vec{y}, \delta)$:
   (a) Compute vector $\vec{z}_\delta$ from $\vec{y}$ and δ by Equation (5).
   (b) Run algorithm $isk_{\vec{z}_\delta} \xleftarrow{R} \text{IKeyGen}(imsk, \vec{z}_\delta)$.
   (c) Return $isk_{\vec{z}_\delta}$.
3. $CT \xleftarrow{R} \text{Enc}(mpk, \vec{x}, m)$:
   (a) Compute vector $\vec{w}$ from $\vec{x}$ by Equation (3).
   (b) Run algorithm $ICT \xleftarrow{R} \text{IEnc}(impk, \vec{w}, m)$.
   (c) Return $CT = ICT$.
4. $\{m, \perp\} \leftarrow \text{Dec}(mpk, t, CT)$:
   (a) Compute $\delta = d(\vec{x}, \vec{y})$.
   (b) If $\delta \in [0, t]$, extracts $isk_{\vec{z}_\delta}$ by running KeyGen algorithm.
   (c) Else return $\perp$.
   (d) Run the decryption algorithm

$$m' = \text{IDec}(impk, isk_{\vec{z}_\delta}, ICT)$$

The ODBE may deviate the definition of DBE defined in Section 4.2 a little bit. However, it can maintain the correctness and security. From the view of correctness, this strategy not only can ensure the correct recovery of message by decryption algorithm, but also can save space cost of storing private key for the decryptor at the same time. From the view of security, we have the following Theorem 3.

Theorem 3. *Our ODBE scheme captures the same security level as the DBE scheme.*

Proof. To show this, we prove that the views of the adversaries in our ODBE and our DBE are equivalent. The view of arbitrary adversary $\mathcal{A}$ are defined as follows:

1. Public parameter mpk.
2. Private key $isk_{\vec{z}_\delta}$ from key extraction oracle.

ACCEPTED MANUSCRIPT

3. Challenged messages m_0^* and m_1^*, and ciphertext CT_b^*.

Clearly, the views of 1) and 3) in DBE and ODBE are equivalent. The view of 2) is also equivalent in DBE and ODBE. Because all the queries to the key extraction oracle are limited by $d(\vec{x}, \vec{y}) > t$, so the views of the adversaries in DBE and ODBE are equivalent. It completes the proof. □

8. Performance analysis

In this section, we present theoretical and experimental performance analysis of our proposals. First, we theoretically analyze the asymptotic time and space complexities of each algorithm of the proposed IPE, and compare it with existing work. Then, we do the some thing for the proposed DBE and ODBE, and compare it with the work in [23]. Finally, we implement our ODBE and the DBE in [23], and present an experimental comparison between them.

8.1. Theoretical analysis

We denote by $\mathcal{P}$ a pairing computation, $\mathcal{E}$ a modular exponentiation computation, $\mathcal{M}$ a multiplication computation and $\mathcal{H}$ a hash computation. Let $|\mathbb{G}|$ be the length of one element in a paring group with a prime group order, and $|\mathbb{G}^c|$ be the length of one element in a paring group with a composite group order. (For simplicity, we assume that $|\mathbb{Z}_p| = |\mathbb{G}_T| = |\mathbb{G}|$ and $|\mathbb{Z}_p^c| = |\mathbb{G}_T^c| = |\mathbb{G}^c|$)

8.1.1. Inner-product encryption

We now compare our proposed IPE scheme with previous work from two aspects: time complexity and space complexity. Table 1 summarizes the analytical results.

Table 1: Comparison with previous inner-product encryption schemes

		[29]	[41]	[40]	[7]	[39]	[39]	[23]	Our Scheme
Time	Setup	$(2n+1)\mathcal{P}^c$	$(4n+5)\mathcal{E}$	$(25n+3)\mathcal{E}+\mathcal{P}$	$(n+11)\mathcal{E}$	$(16n+3)\mathcal{E}+\mathcal{P}$	$(16n+3)\mathcal{E}$	$(n+1)\mathcal{E}+\mathcal{P}$	$(n+2)\mathcal{E}+\mathcal{P}$
	KeyGen	$(4n+1)\mathcal{P}^c$	$(13n+1)\mathcal{E}$	$(15n+2)\mathcal{E}$	$(4n+11)\mathcal{E}$	$n\mathcal{M}$	$(15n+9)\mathcal{E}$	$2\mathcal{E}+n\mathcal{M}$	$(2n+3)\mathcal{E}$
	Enc	$(4n+2)\mathcal{E}^c$	$(12n+3)\mathcal{E}$	$(6n+2)\mathcal{E}$	$(n+3)\mathcal{E}$	$(10n+8)\mathcal{E}$	$(4n+2)\mathcal{E}$	$(2n+2)\mathcal{E}$	$(n+3)\mathcal{E}$
	Dec	$(2n+1)\mathcal{P}^c$	$(4n+2)\mathcal{P}$	$(5n-5)\mathcal{E}+11\mathcal{P}$	$n\mathcal{E}+2\mathcal{P}$	$4(n-1)\mathcal{E}+9\mathcal{P}$	$4(n-1)\mathcal{E}+9\mathcal{P}$	$n\mathcal{E}+2\mathcal{P}$	$n\mathcal{E}+2\mathcal{P}$
Space	Master Key	$(2n+4)\lvert\mathbb{G}^c\rvert$	$(8n+6)\lvert\mathbb{G}\rvert$	$(5n-1)\lvert\mathbb{G}\rvert$	$(n+2)\lvert\mathbb{G}\rvert$	$(10n+14)\lvert\mathbb{G}\rvert$	$(10n+14)\lvert\mathbb{G}\rvert$	$(n+1)\lvert\mathbb{G}\rvert$	$\lvert\mathbb{G}\rvert$
	Public Key	$(2n+3)\lvert\mathbb{G}^c\rvert$	$(8n+4)\lvert\mathbb{G}\rvert$	$(10n-4)\lvert\mathbb{G}\rvert$	$(n+12)\lvert\mathbb{G}\rvert$	$(20n+21)\lvert\mathbb{G}\rvert$	$(20n+21)\lvert\mathbb{G}\rvert$	$(n+4)\lvert\mathbb{G}\rvert$	$(n+3)\lvert\mathbb{G}\rvert$
	Private Key	$(2n+1)\lvert\mathbb{G}^c\rvert$	$(4n+2)\lvert\mathbb{G}\rvert$	$11\lvert\mathbb{G}\rvert$	$(n+1)\lvert\mathbb{G}\rvert$	$(4n+1)\lvert\mathbb{G}\rvert$	$9\lvert\mathbb{G}\rvert$	$2\lvert\mathbb{G}\rvert$	$(n+2)\lvert\mathbb{G}\rvert$
	Ciphertext	$(2n+2)\lvert\mathbb{G}^c\rvert$	$(4n+3)\lvert\mathbb{G}\rvert$	$(5n+2)\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$	$10\lvert\mathbb{G}\rvert$	$(4n+2)\lvert\mathbb{G}\rvert$	$(n+2)\lvert\mathbb{G}\rvert$	$3\lvert\mathbb{G}\rvert$

Time complexity. The Setup algorithm in our IPE requires $n+2$ modular exponentiation computations and one pairing computation. The KeyGen algorithm requires $2n+3$ modular exponentiation computations. The Enc algorithm is dominated by $n+3$ modular exponentiation computations. The Dec algorithm requires n modular exponentiation computations and two pairing computations.

ACCEPTED MANUSCRIPT

Space complexity. The master key *imsk* only consists of one group elements in $\mathbb{G}$. The public key *impk* is composed of $n+3$ group elements in $\mathbb{G}$. Correspondingly, the size of private key is about $(n+2)|\mathbb{G}|$, and the size of ciphertext is only three-element length in $\mathbb{G}$.

Obviously, our IPE scheme has short ciphertext and it is suitable for network-limited application, while the IPE in [23] has short private key and it is suitable for device-limited application. Although the schemes in [7] and [39] also have short ciphertext, but our work outperforms their work in terms of other aspects, such as the time costs of all algorithms and the space costs of master key and public key.

8.1.2. Distance-based encryption

We also compare our two DBE schemes with [23] from two aspects: time complexity and space complexity. Table 2 summarizes the analytical results.

Table 2: Comparison with previous distance-based encryption schemes

		[23]	DBE	ODBE
Time	Setup	$(2n+3)\mathcal{E}+\mathcal{P}$	$(n+4)\mathcal{E}+\mathcal{P}$	$(n+4)\mathcal{E}+\mathcal{P}$
	KeyGen	$(k_0+1)(2\mathcal{E}+2n\mathcal{M})$	$(2n+7)t\mathcal{E}$	$(2n+7)\mathcal{E}$
	Enc	$(l_0+1)(4n+6)\mathcal{E}$	$(n+5)\mathcal{E}$	$(n+5)\mathcal{E}$
	Dec	$2n\mathcal{E}+2\mathcal{P}$	$(n+2)\mathcal{E}+2\mathcal{P}$	$(3n+9)\mathcal{E}+2\mathcal{P}$
Space	Master Key	$(2n+3)\|\mathbb{G}\|$	$\|\mathbb{G}\|$	$\|\mathbb{G}\|$
	Public Key	$(2n+6)\|\mathbb{G}\|$	$(n+5)\|\mathbb{G}\|$	$(n+5)\|\mathbb{G}\|$
	Private Key	$2(k_0+1)\|\mathbb{G}\|$	$(n+4)t\|\mathbb{G}\|$	$(n+4)\|\mathbb{G}\|$
	Ciphertext	$(l_0+1)(2n+4)\|\mathbb{G}\|$	$3\|\mathbb{G}\|$	$3\|\mathbb{G}\|$

Time complexity. The Setup algorithm in our DBE and ODBE requires $n+4$ modular exponentiation computations and one pairing computation. The KeyGen algorithm requires $2n+7$ modular exponentiation computations in ODBE, and it requires $(2n+7)t$ modular exponentiation computations in our DBE. The Enc algorithm in our DBE and ODBE is dominated by $n+5$ modular exponentiation computations. The Dec algorithm requires $3n+9$ modular exponentiation computations and two pairing computations in ODBE, and it requires $n+2$ modular exponentiation computations and two pairing computations in our DBE.

Space complexity. The master key in our DBE and ODBE only consists of one group element in $\mathbb{G}$, and the public key in our DBE and ODBE is composed of $n+3$ group elements in $\mathbb{G}$. The private key in ODBE requires $n+4$ elements in group $\mathbb{G}$, and in our DBE it requires $(n+4)t$ elements in group $\mathbb{G}$. Finally, the size of ciphertexts in our DBE and ODBE is only three-element length in $\mathbb{G}$.

Obviously, our DBE and ODBE schemes have short ciphertext and they are suitable for network-limited application, while the DBE in [23] has short private key and it is suitable for device-limited application. The time cost of our DBE and ODBE is also lower than that of the DBE in [23]. Besides, if l_0 is small such that $k_0 \geq \frac{n+4}{2}$, the size of the private key in ODBE is asymptotically equal to that in [23].

8.2. Experimental analysis

We now evaluate the performance of our ODBE and the DBE in [23] experimentally. All the following experiments are implemented in C++ programming language and are conducted on an Intel-based i5-2320 personal computer with 3GHz processor and 4GB RAM. In our experiments, we utilize the GNU multiple precision arithmetic (GMP) library [1] and pairing based cryptography (PBC) library version 0.5.14 [2] to do the pairing computation parameterized by a.param. All experimental results represent the mean of 10 trials.

We conduct two groups of experiments. First, we evaluate the time cost of each algorithm in our ODBE and the DBE in [23], then in the second group experiment, we evaluate the space cost of the master key, public key, private key, and the ciphertext respectively by varying the parameters k_0 and t. We set the security parameter $\kappa = 1024$ bits and the dimension of DBE $n = 32$ for all the following experiments.

8.2.1. Time cost evaluation

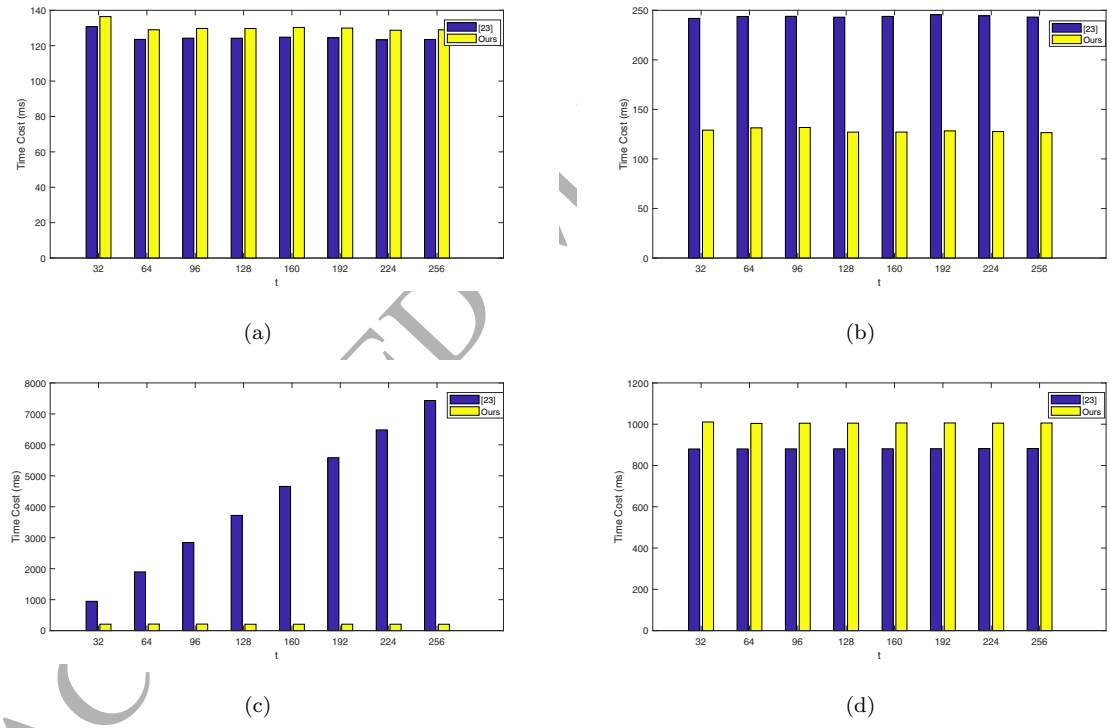


Figure 5: The time cost of each algorithm under different t. (a) The Setup algorithm. (b) The KeyGen algorithm. (c) The Enc algorithm. (d) The Dec algorithm.

In this group of experiments, we evaluate the time cost of each algorithm when the threshold parameter t is set to 32, 64, 96, $\cdots$, 256, other parameters are set constant $k_0 = 16$, $n = 32$, and F is initialized with a symmetric matrix. Figure 5 shows the experimental results. Observed from Figure 5(a), the time cost

of our Setup algorithm is about half of that in [23]. The reason is that the scale factor in our scheme is about 1.0, while it is 2.0 in [23]. For the algorithm KeyGen, our scheme has a slight cost than [23], which is about 7ms. As shown in Figure 5(c), the threshold parameter t does not influence the algorithm Enc in our scheme, which just requires 160+ms for encryption; but in [23], the cost increases with the threshold and requires at least 1000ms when $t = 32$. In Figure 5(d), the decryption cost of both schemes is independent with the increase of parameter threshold t, and cost of our scheme is about 180ms more than that in [23].

8.2.2. Space cost evaluation

Table 3: Space cost (KB) under different t

Algorithm	**DBE in [23]**					**Ours**
	$t = 16$	$t = 32$	$t = 64$	$t = 128$	$t = 256$	$t = 16, 32, 64, 128, 256$
Master key	8.375	8.375	8.375	8.375	8.375	**0.125**
Public key	8.5	8.5	8.5	8.5	8.5	**4.625**
Private Key	**4.25**	**4.25**	**4.25**	**4.25**	**4.25**	4.5
Ciphertext	8.5	17	34	68	136	**0.375**

Table 4: Space cost (KB) under different k_0

Algorithm	**DBE in [23]**				**Ours**
	$k_0 = 32$	$k_0 = 64$	$k_0 = 128$	$k_0 = 256$	$k_0 = 32, 64, 128, 256$
Master key	8.375	8.375	8.375	8.375	**0.125**
Public key	8.5	8.5	8.5	8.5	**4.625**
Private Key	8.25	16.25	32.25	64.25	**4.5**
Ciphertext	68	34	17	8.5	**0.375**

In this group of experiments, we evaluate the space cost of master key, public key, private key, and ciphertext respectively. We first set the threshold parameter t from 16 to 256 by doubling t and other parameters constant, $k_0 = 16$, $n = 32$, and F is initialized with a symmetric matrix. We then set the parameter k_0 from 32 to 256 by doubling k_0 and other parameters constant, $t = 256$, $n = 32$, and F is initialized with a symmetric matrix. Table 3 and Table 4 show the experimental results.

As shown in Table 3, with the change of parameter t, the space cost of master key, public key, and ciphertext in our scheme keeps constant and it is lower than that of the scheme in [23], respectively. The size of ciphertext grows exponentially in [23] and it requires at least 8.5KB when $t = 16$, but our scheme only requires 0.375KB. The size of private key in our scheme is 4.5KB and in [23] it is 4.25KB. Similar results can be observed from Table 4. The space cost of our scheme keeps unchanged with the change of parameter

ACCEPTED MANUSCRIPT

ACCEPTED MANUSCRIPT

k_0. In [23], the master key and the public key are independent of k_0. However, the size of private key grows exponentially with the increasing of k_0 and it requires at least 8.25KB when $k_0 = 32$, which is still higher than ours. The ciphertext size decreases exponentially with the parameter k_0, but it is still much higher than ours when $k = 256$.

8.2.3. Overall comparison

Finally, we normalize all eight indicators considered in our experiments (i.e. the time cost of Setup, KeyGen, Enc, Dec and the space cost of master key, public key, private key, and ciphertext) into the range [0.1, 10] by letting the best score be 10 and the worst score 0.1. Then we plot the radar chart of these normalized eight indicators in Figure 6, which gives an overall comparison between our ODBE and the DBE in [23]. The area size of the closed curve can be used to measure the overall performance of the scheme: the larger, the better. Clearly, our scheme has a better overall performance than the work in [23].

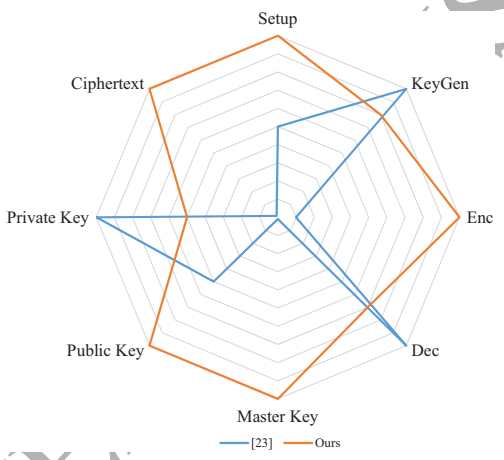


Figure 6: The radar chart of normalized eight indicators.

9. Conclusion

In this paper, we design a biometric identity-based encryption (BIBE) by constructing a time-saving and space-saving distance-based encryption (DBE), where Mahalanobis distance serves as the measurement tool for determining whether two biometrics information belongs to the same user. Leveraging the symmetric property of the covariance matrix, we build a vector transform between the DBE and the inner-product encryption (IPE). We propose an inner product encryption (IPE) scheme that has short ciphertext. Based on the IPE, we construct a provable-secure DBE with short ciphertext. Furthermore, we optimize the proposed DBE such that it also has short private key, the optimized version is called ODBE. We prove that the proposed IPE is secure under selective identity, adaptive chosen-plaintext attack (IND-sID-CPA), and our DBE and ODBE capture the same security with the IPE according to the security reduction. Our

ACCEPTED MANUSCRIPT

theoretical analysis in terms of time, space and communication complexities shows the superiority of the proposed IPE, DBE and ODBE over existing work, and our extensive experimental results validate the theoretical analysis and demonstrate the effectiveness and efficiency of our proposal.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61672118) and Graduate Scientific Research and Innovation Foundation of Chongqing, China (No. CYB16046).

References

[1] GNU: the GNU multiple precision arthmetic library, https://gmplib.org/.

[2] PBC: the pairing-based cryptography library version 0.5.14, http://crypto.stanford.edu/pbc/.

[3] M. Abdalla, F. Bourse, A. D. Caro, D. Pointcheval, Simple functional encryption schemes for inner products, in: Public Key Cryptography (PKC), 2015, pp. 733–751.

[4] S. Agrawal, S. Agrawal, S. Badrinarayanan, A. Kumarasubramanian, M. Prabhakaran, A. Sahai, On the practical security of inner product functional encryption, in: Public Key Cryptography (PKC), 2015, pp. 777–798.

[5] S. Agrawal, X. Boyen, V. Vaikuntanathan, P. Voulgaris, H. Wee, Functional encryption for threshold functions (or fuzzy ibe) from lattices, in: Public Key Cryptography (PKC), 2012, pp. 280–297.

[6] S. Agrawal, D. M. Freeman, V. Vaikuntanathan, Functional encryption for inner product predicates from learning with errors, in: ASIACRYPT, 2011, pp. 21–40.

[7] N. Attrapadung, B. Libert, Functional encryption for inner product: Achieving constant-size ciphertexts with adaptive security or support for negation, in: Public Key Cryptography (PKC), 2010, pp. 384–402.

[8] M. Bellare, P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, in: Proc. ACM Conference on Computer and Communications Security (CCS), 1993, pp. 62–73.

[9] D. Boneh, X. Boyen, E.-J. Goh, Hierarchical identity based encryption with constant size ciphertext, in: EUROCRYPT, 2005, pp. 440–456.

[10] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, in: CRYPTO, 2001, pp. 213–229.

[11] D. Boneh, A. Sahai, B. Waters, Functional encryption: Definitions and challenges, in: Theory of Cryptography (ToC), 2011, pp. 253–273.

[12] D. Boneh, B. Waters, Conjunctive, subset, and range queries on encrypted data, in: Theory of Cryptography (ToC), 2007, pp. 535–554.

[13] X. Boyen, B. Waters, Anonymous hierarchical identity-based encryption (without random oracles), in: CRYPTO, 2006, pp. 290–307.

[14] A. Castiglione, K.-K. R. Choo, M. Nappi, F. Narducci, Biometrics in the cloud: Challenges and research opportunities, IEEE Cloud Computing 4 (4) (2017) 12–17.

[15] F. Chen, T. Xiang, Y. Yang, S. S. M. Chow, Secure cloud storage meets with secure network coding, IEEE Transactions on Computers, preprint 65 (6) (2016) 1936–1948.

[16] J. Chen, Y. Wang, X. Wang, On-demand security architecture for cloud computing, Computer (7) (2012) 73–78.

[17] J. Chen, G. Wu, Z. Ji, Secure interoperation of identity managements among different circles of trust, Computer Standards & Interfaces 33 (6) (2011) 533–540.

[18] J. Chen, G. Wu, L. Shen, Z. Ji, Differentiated security levels for personal identifiable information in identity management system, Expert Systems with Applications 38 (11) (2011) 14156–14162.

ACCEPTED MANUSCRIPT

[19] G. I. Davida, Y. Frankel, B. J. Matt, On enabling secure applications through off-line biometric identification, in: IEEE Symposium on Security and Privacy (S&P), 1998, pp. 148–157.

[20] G. S. Eskander, R. Sabourin, E. Granger, A bio-cryptographic system based on offline signature images, Information Sciences 259 (2014) 170–191.

[21] S. Goldwasser, Y. Kalai, R. A. Popa, V. Vaikuntanathan, N. Zeldovich, Reusable garbled circuits and succinct functional encryption, in: Proc. annual ACM Symposium on Theory Of Computing (STOC), 2013, pp. 555–564.

[22] F. Guo, W. Susilo, Y. Mu, Poster: Euclidean distance based encryption: How to embed fuzziness in biometric based encryption, in: Proc. ACM Conference on Computer and Communications Security (CCS), 2014, pp. 1430–1432.

[23] F. Guo, W. Susilo, Y. Mu, Distance-based encryption: How to embed fuzziness in biometric-based encryption, IEEE Transactions on Information Forensics and Security 11 (2) (2016) 247–257.

[24] J. Horwitz, B. Lynn, Toward hierarchical identity-based encryption, in: EUROCRYPT, 2002, pp. 466–481.

[25] T. Ignatenko, F. M. Willems, Biometric systems: Privacy and secrecy aspects, IEEE Transactions on Information Forensics and Security 4 (4) (2009) 956–973.

[26] G. Iovane, C. Bisogni, L. D. Maio, M. Nappi, An encryption approach using information fusion techniques involving prime numbers and face biometrics, IEEE Transactions on Sustainable Computing DOI: 10.1109/TSUSC.2018.2793466.

[27] S. Islam, A. K. Das, M. K. Khan, Design of a provably secure identity-based digital multi-signature scheme using biometrics and fuzzy extractor, Security and Communication Networks 9 (16) (2016) 3229–3238.

[28] S. M. M. Jr, M. Peyravian, A. L. Roginsky, N. Zunic, Biometric based multi-party authentication, US Patent 6,697,947 (Feb. 24 2004).

[29] J. Katz, A. Sahai, B. Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, in: EUROCRYPT, 2008, pp. 146–162.

[30] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, B. Waters, Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, in: EUROCRYPT, 2010, pp. 62–91.

[31] J. Li, X. Li, L. Wang, D. He, H. Ahmad, X. Niu, Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption, Soft Computing 22 (3) (2018) 707–714.

[32] X. Li, M. H. Ibrahim, S. Kumari, A. K. Sangaiah, V. Gupta, K.-K. R. Choo, Anonymous mutual authentication and key agreement scheme for wearable sensors in wireless body area networks, Computer Networks 129 (2017) 429–443.

[33] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, S. Kumari, A robust ECC based provable secure authentication protocol with privacy protection for industrial internet of things, IEEE Transactions on Industrial Informatics DOI: 10.1109/TII.2017.2773666.

[34] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, K.-K. R. Choo, A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments, Journal of Network and Computer Applications 103 (2018) 194–204.

[35] X. Li, J. Niu, J. Liao, W. Liang, Cryptanalysis of a dynamic identity-based remote user authentication scheme with verifiable password update, International Journal of Communication Systems 28 (2) (2015) 374–382.

[36] R. Á. Mariño, F. H. Álvarez, L. H. Encinas, A crypto-biometric scheme based on iris-templates with fuzzy extractors, Information Sciences 195 (2012) 91–102.

[37] D. Nali, C. M. Adams, A. Miri, Using threshold attribute-based encryption for practical biometric-based access control., Internatonal Journal Network Security 1 (3) (2005) 173–182.

[38] K. Nandakumar, A. K. Jain, S. Pankanti, Fingerprint-based fuzzy vault: Implementation and performance, IEEE Transactions on Information Forensics and Security 2 (4) (2007) 744–757.

[39] T. Okamoto, K. Takashima, Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption, in: Cryptology And Network Security (CANS), 2011, pp. 138–159.

ACCEPTED MANUSCRIPT

[40] T. Okamoto, K. Takashima, Adaptively attribute-hiding (hierarchical) inner product encryption, in: EUROCRYPT, 2012, pp. 591–608.

[41] J. H. Park, Inner-product encryption under standard assumptions, Designs, Codes and Cryptography 58 (3) (2011) 235–257.

[42] A. Sahai, B. Waters, Fuzzy identity-based encryption, in: Advances in EUROCRYPT, 2005, pp. 457–473.

[43] N. D. Sarier, Multimodal biometric identity based encryption, Future Generation Computer Systems 80 (2018) 112–125.

[44] W. J. Scheirer, T. E. Boult, Cracking fuzzy vaults and biometric encryption, in: Biometrics Symposium, 2007, pp. 1–6.

[45] J. H. Seo, T. Kobayashi, M. Ohkubo, K. Suzuki, Anonymous hierarchical identity-based encryption with constant size ciphertexts, in: Public Key Cryptography (PKC), 2009, pp. 215–234.

[46] A. Shamir, Identity-based cryptosystems and signature schemes, in: CRYPTO, 1985, pp. 47–53.

[47] B. Wang, B. Li, H. Li, Panda: Public auditing for shared data with efficient user revocation in the cloud, IEEE Transactions on Services Computing 8 (1) (2015) 92–106.

[48] H. Wang, D. He, J. Shen, Z. Zheng, X. Yang, M. H. Au, Fuzzy matching and direct revocation: a new CP-ABE scheme from multilinear maps, Soft Computing 22 (7) (2018) 2267–2274.

[49] B. Waters, Efficient identity-based encryption without random oracles, in: EUROCRYPT, 2005, pp. 114–127.

[50] B. Waters, Functional encryption for regular languages, in: CRYPTO, 2012, pp. 218–235.

[51] C. Zhang, L. Zhu, C. Xu, Ptbi: An efficient privacy-preserving biometric identification based on perturbed term in the cloud, Information Sciences 409 (2017) 56–67.

ACCEPTED MANUSCRIPT