More Efficient Constructions for Inner-Product Encryption

Somindu C. Ramanna(✉)

Laboratoire LIP, ENS de Lyon, Lyon, France
somindu.ramanna@ens-lyon.fr

Abstract. We propose new constructions for inner product encryption – $\mathcal{IPE}_1$ and $\mathcal{IPE}_2$, both secure under the eXternal Diffie-Hellman assumption (SXDH) in asymmetric pairing groups. The first scheme has constant-size ciphertexts whereas the second one is weakly attribute hiding. $\mathcal{IPE}_2$ is derived from the identity-based encryption scheme of Jutla Roy (Asiacrypt 2013), that was extended from tag-based quasi-adaptive non-interactive zero-knowledge (QA-NIZK) proofs for linear subspaces of vector spaces over bilinear groups. The verifier common reference string (CRS) in these tag-based systems are split into two parts, that are combined during verification. We consider an alternate form of the tag-based QA-NIZK proof with a single verifier CRS that already includes a tag, different from the one defining the language. The verification succeeds as long as the two tags are unequal. Essentially, we embed a two-equation revocation mechanism in the verification. The new QA-NIZK proof system leads to $\mathcal{IPE}_1$, a constant-sized ciphertext IPE scheme with very short ciphertexts. Both the IPE schemes are obtained by applying the n-equation revocation technique of Attrapadung and Libert (PKC 2010) to the corresponding identity based encryption schemes and proved secure under SXDH assumption. As an application, we show how our schemes can be specialised to obtain the first fully secure identity-based broadcast encryption based on SXDH with a trade-off among the public parameters, ciphertext and key sizes, all of them being sub-linear in the maximum number of recipients of a broadcast.

Keywords: Inner-product encryption · Attribute-hiding · Constant-size ciphertexts · Quasi-adaptive non-interactive zero knowledge proofs

1 Introduction

Inner product encryption (IPE) is a special form of the more general attribute-based encryption (ABE), which provides fine-grained access control to encrypted data. In ABE, a ciphertext is encrypted to some attribute $\mathbf{x}$ and a secret key is associated to some attribute $\mathbf{y}$ such that decryption succeeds iff some relation R on $\mathbf{x}, \mathbf{y}$ holds true i.e., $R(\mathbf{x}, \mathbf{y}) = 1$. The standard notion of security for ABE requires resistance to collusion attacks. More precisely, the privacy of a message encrypted to attribute $\mathbf{x}$ must not be compromised in the event of an attack by a group of users possessing secret keys for $\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_q$ where

M. Manulis et al. (Eds.): ACNS 2016, LNCS 9696, pp. 231–248, 2016.
DOI: 10.1007/978-3-319-39555-5_13

$R(\mathbf{x}, \mathbf{y}_i) = 0$ for all $i = 1, \ldots, q$. Another useful security property, called *weak attribute hiding*, requires that given a ciphertext, the group of corrupt users unauthorised to decrypt the ciphertext, learn nothing about the attribute $\mathbf{x}$. In both cases, *adaptive security* allows users to be corrupted adaptively.

A simple form of ABE is identity-based encryption, where $\mathbf{x}$ and $\mathbf{y}$ represent identities and the relation R tests equality of identities. IPE is a more complex form with R testing orthogonality of $\mathbf{x}$ and $\mathbf{y}$ that are vectors in some inner product space. In other words, $R(\mathbf{x}, \mathbf{y}) = 1$ if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ and 0 otherwise. Though they appear restricted, inner products cover a wide range of functionalities useful in practice including polynomial functions, boolean formulae evaluating conjunctive and disjunctive normal forms, and identity-based broadcast encryption and revocation.

Most efficient constructions of IPE are based on pairings. A pairing $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ is a bilinear, non-degenerate and efficiently computable map defined over three groups $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ all having the same order. The common order of the groups may be composite or prime. Prime order pairings where $\mathbb{G}_1 \neq \mathbb{G}_2$ are called asymmetric. The best choices for implementation are *asymmetric pairings*, particularly those with no efficiently computable isomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$ (called *Type-3 pairings*), from a point of view of security as well as efficiency. A consequence of the absence of efficient isomorphisms makes the decisional Diffie-Hellman (DDH) problem hard in both groups $\mathbb{G}_1$ and $\mathbb{G}_2$, collectively called the symmetric eXternal decisional Diffie-Hellman (SXDH) problem. We mainly focus on security under this assumption.

A powerful technique to obtain adaptive security for attribute-based encryption schemes is the dual system methodology introduced by Waters [Wat09]. Important features of the underlying algebraic structure that facilitate a dual system proof are *cancelling* and *parameter-hiding*. These features are explicitly available in composite order pairing groups that are not really suitable for practical deployment. A number of works have investigated the possibilities of translating the properties of composite order pairings to the prime-order setting, mostly in the context of dual system hierarchical IBE and ABE. However, the constructions resulting from these translations are not necessarily optimised in terms of various system parameters (such as ciphertext/key size, time required for decryption and so on). In contrast, direct constructions in the prime-order setting circumventing the route via composite order pairings, holds more promise in this regard. We believe that IPE as a cryptographic primitive is significant enough to justify attempts for direct constructions.

The goal of this work is to obtain new direct Type-3 pairing-based constructions of IPE that are efficient, adaptively secure with a focus on achieving either of the following properties – attribute-hiding or compact ciphertexts – from the SXDH assumption.

Our Contributions. We propose two new IPE schemes based on prime-order pairings named $\mathcal{IPE}_1$ and $\mathcal{IPE}_2$ – the former with constant-sized ciphertexts and the latter achieving weak attribute hiding, both secure under the SXDH assumption. The constructions are derived from quasi-adaptive non-interactive

Table 1. Constant-size ciphertext IPE.

Scheme	#pp	#cpr	#key	#dec
[CGW15]	$(2n+4)\vert\mathbb{G}_1\vert + \vert\mathbb{G}_T\vert$	$4\vert\mathbb{G}_1\vert + \vert\mathbb{G}_T\vert$	$(2n+2)\vert\mathbb{G}_2\vert$	$4[\mathrm{P}] + 2n[\mathrm{M}_2]$
$\mathcal{IPE}_1$	$(n+3)\vert\mathbb{G}_1\vert + \vert\mathbb{G}_T\vert$	$3\vert\mathbb{G}_1\vert + \vert\mathbb{Z}_p\vert + \vert\mathbb{G}_T\vert$	$(2n+1)\vert\mathbb{G}_2\vert + (n-1)\vert\mathbb{Z}_p\vert$	$3[\mathrm{P}]+(2n-2)[\mathrm{M}_2]+[\mathrm{E}]$

Table 2. Attribute-hiding IPE.

Scheme	#pp	#cpr	#key	#dec
[CGW15]	$(2n+4)\vert\mathbb{G}_1\vert + \vert\mathbb{G}_T\vert$	$(2n+2)\vert\mathbb{G}_1\vert + \vert\mathbb{G}_T\vert$	$4\vert\mathbb{G}_2\vert$	$4[\mathrm{P}] + 2n[\mathrm{M}_1]$
$\mathcal{IPE}_2$	$(n+3)\vert\mathbb{G}_1\vert + \vert\mathbb{G}_T\vert$	$(n+1)\vert\mathbb{G}_1\vert + (n-1)\vert\mathbb{Z}_p\vert + \vert\mathbb{G}_T\vert$	$5\vert\mathbb{G}_2\vert$	$3[\mathrm{P}] + (n+1)[\mathrm{M}_1]$

zero knowledge (QA-NIZK) proofs of Jutla and Roy [JR13] and an IBE proposed in the same work (denoted $\mathcal{JR}$-$\mathcal{IBE}$ in the rest of the paper). $\mathcal{IPE}_2$ is obtained from $\mathcal{JR}$-$\mathcal{IBE}$ by a novel application of the n-equation revocation technique of Attrapadung and Libert [AL10]. But a constant-size ciphertext IPE cannot be constructed in a similar way from $\mathcal{JR}$-$\mathcal{IBE}$. To get around this problem, we propose a small tweak to the Jutla-Roy QA-NIZK proofs that leads to an alternate form of $\mathcal{JR}$-$\mathcal{IBE}$ (named $\mathcal{JR}$-$\mathcal{IBE}$-$\mathcal{D}$). The n-equation revocation method is then combined with $\mathcal{JR}$-$\mathcal{IBE}$-$\mathcal{D}$ to construct $\mathcal{IPE}_1$. QA-NIZK proofs were only known to yield IBE [JR13], hierarchical IBE (HIBE) [RS14b] and identity-based broadcast encryption [RS14a] but the question of whether they are useful in constructing other forms of ABE remained open. Thus, we (partially) settle an open question posed in [CGW15].

Tables 1 and 2 compare our constructions to those recently proposed by Chen et al. [CGW15]. The reason we do not include other previous constructions in the comparison is that the constructions in [CGW15] are the most efficient instantiations known so far and their constructions achieve security from the SXDH assumption. First, we define some abbreviations/notation we use in the comparison. #pp, #cpr and #key denote the sizes of public parameters, ciphertexts and keys respectively. #dec denotes the time required for decryption. $|X|$ denotes the size of representation of an element from X. [P], [M$_i$] (for $i = 1, 2$) and [E] respectively denote the time required for pairing operation, scalar multiplication in $\mathbb{G}_i$ (for $i = 1, 2$) and exponentiation in $\mathbb{G}_T$ respectively.

Note that both our schemes are at least as efficient as the corresponding instantiations in [CGW15]. The public parameters and decryption time are better in our schemes. The ciphertext size in both $\mathcal{IPE}_1$ and $\mathcal{IPE}_2$ are at least as short as those in [CGW15].

Quasi-Adaptive NIZK Proofs to IPE. Jutla and Roy [JR13] proposed constructions of quasi-adaptive non-interactive zero knowledge (QA-NIZK) proofs for linear equations over pairing groups that have a weaker soundness criterion called quasi-adaptive soundness. The difference with regular NIZKs is that the common reference string (CRS) is allowed to depend on the language.

These are useful in constructing a number of primitives, such as signatures, CCA2-secure public key encryption, commitment schemes and so on. From the signature scheme, they obtained an IBE using Naor's transform, which is the most efficient IBE known till date in terms of size of public parameters and ciphertexts achieving adaptive security under standard assumptions. Building upon this IBE, we obtain a weakly attribute hiding IPE scheme using the n-equation revocation method proposed in [AL10].

The NIZK construction that leads to the IBE is actually a split-CRS NIZK for tag-based languages, where the CRS for the verifier is split into two components. These two components are then combined using a public random tag ctag, which is also a parameter defining the language. We make a slight modification by combining the two components of the split-CRS with another tag ktag and only providing the combination as the CRS. This ensures that verification is successful unless the two tags are equal, thus making unconditional failure of verification a possibility. Nevertheless, the probability of failure is negligible and this small modification leads to an IBE scheme that has tags in both ciphertexts and keys. Decryption requires the two-equation revocation technique of Sahai and Waters [LSW08] as used in Waters' IBE [Wat09] and fails unconditionally with (negligible) probability equal to that of NIZK verification failure. The resulting IBE which we denote as $\mathcal{JR}$-$\mathcal{IBE}$-$\mathcal{D}$, allows extension to primitives that were not possible from $\mathcal{JR}$-$\mathcal{IBE}$, such as identity-based revocation schemes with small secret keys, constant-size ciphertext IBBE and so on. We present a construction of constant-size ciphertext IPE that can then be specialised to the afore-mentioned primitives. Unlike earlier constructions based on dual pairing vector spaces, specialising the IPE to specific cases actually leads to optimal constructions, i.e., these schemes are as efficient as direct constructions obtained from $\mathcal{JR}$-$\mathcal{IBE}$-$\mathcal{D}$.

The reason for first constructing an IBE is two-fold. Firstly, it provides better intuition and acts as a basis for moving to inner product functionality. Second and most importantly, we do not know a direct generic transformation from QA-NIZK proofs to IBE, let alone IPE. To this end, there has been some recent work [JR15] that defines the so-called dual system simulation sound QA-NIZK proofs that explain the $\mathcal{JR}$-$\mathcal{IBE}$ construction better in generic terms. It may be possible to explain our constructions too within this framework.

Application. As an application of IPE, we consider identity-based broadcast encryption (IBBE) wherein the goal is to securely broadcast an encrypted message to users associated with identities so that only a subset of *privileged* users can decrypt the message. Unlike the public key broadcast setting where the number of public keys varies polynomially with the security parameter, the number of valid identities in an IBBE are allowed to be exponential. Some direct constructions of adaptively secure constructions of IBBE schemes already exist in the literature [GW09, AL10, RS14a]. Most of these schemes require the number of privileged recipients for any broadcast to be bounded during setup (call this bound n). Previous schemes had either constant-sized ciphertexts or constant-sized keys with at least one out of public parameters, ciphertext, key having size depending linearly on n.

We show how to construct an IBBE from $\mathcal{IPE}_1$ that achieves parameters, ciphertexts and keys all having size sublinear in n while maintaining security under static complexity assumptions. (Here, static means that the number of elements in instance is a constant). Due to lack of space, we present this discussion in the full version of this paper [Ram16].

Related Work. There have been several constructions of attribute encryption schemes based on pairings [SW05, GPSW06, OSW07, BSW07, Wat11, LW12], some focussing only on inner product encryption [KSW08, OT09, OT10, AL10]. Lattice-based constructions include ABE of [Boy13] for formulas and [GVW13, GGH+13] for circuits. We are mostly interested in constructions based on bilinear maps with prime order. Several approaches have been taken to constructing ABE schemes in the prime order pairing setting, most of them attempting to simulate properties of composite order pairings in suitably defined prime-order counterparts. A widely used technique is based on dual pairing vector spaces [OT08, OT09] which obtains all the nice theoretical properties but fails to preserve efficiency. The sparse DPVS technique introduced in [OT11] uses subgroups of sparse matrices (those mostly covered with zero entries) with the hope of improving efficiency. But the conversions are no longer generic and involve very complex security analysis. Another generic technique is that of dual system groups [CW13] that provides more efficient translations in the context of IBE. However, it does not extend to primitives that require anonymity or attribute-hiding. Two recent works [Wee14, Att14] present unifying frameworks for predicate encryption schemes fully secure within the dual system framework. These frameworks were defined in the composite order setting and later translated to prime-order groups [CGW15, Att15]. The new technique used in [CGW15] actually obtained very efficient and near-optimal constructions in the prime-order setting. Apart from translations from composite-order groups, there have been attempts at direct constructions of certain simple primitives such as IBE and HIBE. The approach of [JR13] is via QA-NIZK proofs. This was later extended to HIBE in [RS14b] and IBBE [RS14a]. Another interesting approach was to construct (H)IBE from message authentication codes (which is a symmetric primitive), examined in [BKP14]. But we do not know whether the last method extends to attribute-based encryption.

2 Preliminaries

This section introduces some notation followed by a review of pairings and related hardness assumptions. Also provided are definitions related to inner-product encryption.

2.1 Notation

The notation $x_1, \ldots, x_k \xleftarrow{\mathrm{R}} \mathcal{X}$ indicates that elements $x_1, \ldots, x_k$ are sampled independently from the set $\mathcal{X}$ according to some distribution R. We use U to denote the uniform distribution. For a (probabilistic) algorithm $\mathcal{A}$, $y \xleftarrow{\mathrm{R}} \mathcal{A}(x)$ means that y is chosen according to the output distribution of $\mathcal{A}$ on input x. $\mathcal{A}(x; r)$ denotes that $\mathcal{A}$ is run on input x with its internal random coins set to r. For two integers $a < b$, the notation $[a, b]$ represents the set $\{x \in \mathbb{Z} : a \leq x \leq b\}$. If $\mathbb{G}$ is a finite cyclic group, then $\mathbb{G}^{\times}$ denotes the set of generators of $\mathbb{G}$.

We denote vectors in $\mathbb{Z}_p^n$ by bold upright characters (e.g. $\mathbf{x}$). Inner product of two $\mathbb{Z}_p^n$-vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ is given by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^{n} x_i y_i$.

2.2 Asymmetric Pairings and Hardness Assumptions

A bilinear pairing ensemble is a 7-tuple $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1, P_2)$ where $\mathbb{G}_1 = \langle P_1 \rangle$, $\mathbb{G}_2 = \langle P_2 \rangle$ are written additively and $\mathbb{G}_T$ is a multiplicatively written group, all having the same order p and $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ (the pairing) is a bilinear, non-degenerate and efficiently computable map. In a Type-3 pairing, $\mathbb{G}_1 \neq \mathbb{G}_2$ and no efficiently computable isomorphisms between $\mathbb{G}_1$ and $\mathbb{G}_2$ are known. The constructions we provide are based on such pairings.

The assumptions based on which the security of our constructions is proven are the decision Diffie-Hellman (DDH) assumptions in groups $\mathbb{G}_1$ and $\mathbb{G}_2$, called DDH1 and DDH2 respectively. Below, we describe these two assumptions. Technically speaking, the two assumptions are not in the standard form but can be shown to be equivalent. The reason we use the alternate forms is that they suit the requirements of our reductions and also to be in sync with the notation in [JR13].

Let $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1, P_2)$ be an asymmetric pairing ensemble and $\mathscr{A}$, a probabilistic polynomial time (PPT) algorithm $\mathscr{A}$ that outputs 0 or 1.

Assumption DDH1. Define a distribution $\mathcal{D}$ as follows: $P_1 \xleftarrow{\mathrm{U}} \mathbb{G}_1^{\times}$; $b, s \xleftarrow{\mathrm{U}} \mathbb{Z}_p$, $\mu \xleftarrow{\mathrm{U}} \mathbb{Z}_p$; $\mathcal{D} = (\mathcal{G}, P_1, bP_1, bsP_1)$. The advantage of $\mathscr{A}$ in solving the DDH1 problem is given by

$$\mathsf{Adv}_{\mathcal{G}}^{\mathrm{DDH1}}(\mathscr{A}) = |\Pr[\mathscr{A}(\mathcal{D}, sP_1) = 1] - \Pr[\mathscr{A}(\mathcal{D}, (s + \mu)P_1) = 1]|.$$

Essentially, $\mathscr{A}$ has to decide whether $\mu = 0$ or $\mu \in_{\mathrm{U}} \mathbb{Z}_p$ given $(\mathcal{D}, (s + \mu)P_1)$. The (ε, t)-DDH1 assumption holds in $\mathcal{G}$ if for any adversary $\mathscr{A}$ running in time at most t, $\mathsf{Adv}_{\mathcal{G}}^{\mathrm{DDH1}}(\mathscr{A}) \leq \varepsilon$.

Assumption DDH2. Let a distribution $\mathcal{D}$ be defined as follows: $P_2 \xleftarrow{\mathrm{U}} \mathbb{G}_2^{\times}$, $r, c \xleftarrow{\mathrm{U}} \mathbb{Z}_p$, $\gamma \xleftarrow{\mathrm{U}} \mathbb{Z}_p$;

$$\mathcal{D} = (\mathcal{G}, P_2, rP_2, cP_2).$$

$\mathscr{A}$'s advantage in solving the DDH2 problem is given by

$$\mathsf{Adv}_{\mathcal{G}}^{\mathrm{DDH2}}(\mathscr{A}) = |\Pr[\mathscr{A}(\mathcal{D}, rcP_2) = 1] - \Pr[\mathscr{A}(\mathcal{D}, (rc + \gamma)P_2) = 1]|.$$

The (ε, t)-DDH2 assumption is that, for any t-time algorithm $\mathscr{A}$, $\mathsf{Adv}_{\mathcal{G}}^{\mathrm{DDH2}}(\mathscr{A}) \leq \varepsilon$.

2.3 Inner Product Encryption (IPE)

Definition 1 (IPE). *Let V denote a vector space of dimension n over a field $\mathbb{F}$ and $\mathcal{M}$ denote the message space. An IPE scheme for inner products over V, is defined by four probabilistic algorithms –* Setup*,* $\mathsf{Encrypt}$*,* KeyGen *and* $\mathsf{Decrypt}$*.*

$\mathsf{Setup}(\kappa, n)$ *Takes as input a security parameter κ and the dimension of V. It outputs the public parameters $\mathcal{PP}$ and the master secret $\mathcal{MSK}$.*

$\mathsf{KeyGen}(\mathcal{MSK}, \mathbf{y})$ *On input a vector $\mathbf{y} \in V$ and the master secret $\mathcal{MSK}$; this algorithm outputs a secret key $\mathcal{SK}_{\mathbf{y}}$ for $\mathbf{y}$.*

$\mathsf{Encrypt}(\mathcal{PP}, m, \mathbf{x})$ *Takes as input a message m and an attribute vector $\mathbf{x} \in V$ and outputs a ciphertext $\mathcal{C}$.*

$\mathsf{Decrypt}(\mathcal{PP}, \mathcal{C}, \mathcal{SK}_{\mathbf{y}})$ *If $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, this algorithm returns the message m and $\perp$ otherwise.*

Correctness. The IPE scheme is said to satisfy the correctness condition if for all vectors $\mathbf{x}, \mathbf{y} \in V$ with $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ and for all $m \in \mathcal{M}$, if $(\mathcal{PP}, \mathcal{MSK}) \xleftarrow{\text{R}} \mathsf{Setup}(\kappa, n)$, $\mathcal{SK}_{\mathbf{y}} \xleftarrow{\text{R}} \mathsf{KeyGen}(\mathcal{MSK}, \mathbf{y})$, $\mathcal{C} \xleftarrow{\text{R}} \mathsf{Encrypt}(\mathcal{PP}, m, \mathbf{x})$, then $\Pr[m = \mathsf{Decrypt}(\mathcal{PP}, \mathcal{C}, \mathcal{SK}_{\mathbf{y}})] = 1$.

Definition 2 (Security). *The security definition for inner product encryption scheme that we consider is weak attribute hiding and adaptive security against chosen plaintext attacks. It is formalised in terms of the following game* $\mathsf{ind\text{-}wah\text{-}cpa}$ *between an adversary $\mathscr{A}$ and a challenger.*

Setup: *The challenger runs the* Setup *algorithm of the IPE and gives the public parameters to $\mathscr{A}$.*

Key Extraction Phase 1: *$\mathscr{A}$ makes a number of key extraction queries adaptively. For a query on a vector $\mathbf{y}$, the challenger responds with a key $\mathcal{SK}_{\mathbf{y}}$.*

Challenge: *$\mathscr{A}$ provides two pairs of messages and attribute vectors $m_0, \widehat{\mathbf{x}}_0$ and $m_1, \widehat{\mathbf{x}}_1$with the restriction that if $\mathbf{y}$ is queried in the key extraction phase 1, then $\langle \widehat{\mathbf{x}}_0, \mathbf{y} \rangle \neq 0$ and $\langle \widehat{\mathbf{x}}_1, \mathbf{y} \rangle \neq 0$. The challenger chooses a bit β uniformly at random from $\{0, 1\}$, encrypts m_β to $\widehat{\mathbf{x}}_\beta$ and returns the resulting ciphertext $\widehat{\mathcal{C}}$ to $\mathscr{A}$.*

Key Extraction Phase 2: *$\mathscr{A}$ makes more key extraction queries with the restriction that it cannot query a key for any vector $\mathbf{y}$ with $\langle \widehat{\mathbf{x}}_0, \mathbf{y} \rangle = 0$ or $\langle \widehat{\mathbf{x}}_1, \mathbf{y} \rangle = 0$.*

Guess: *$\mathscr{A}$ outputs a bit β'.*

If $\beta = \beta'$, then $\mathscr{A}$ wins the game. The advantage of $\mathscr{A}$ in winning the $\mathsf{ind\text{-}wah\text{-}cpa}$ *is given by*

$$\mathsf{Adv}_{\mathrm{IPE}}^{\mathsf{ind\text{-}wah\text{-}cpa}}(\mathscr{A}) = \left| \Pr[\beta = \beta'] - \frac{1}{2} \right|.$$

The IPE scheme is said to be (ε, t, q)-$\mathsf{IND\text{-}WAH\text{-}CPA}$ *secure if every t-time adversary making at most q key extraction queries has $\mathsf{Adv}_{\mathrm{IPE}}^{\mathsf{ind\text{-}wah\text{-}cpa}}(\mathscr{A}) \leq \varepsilon$.*

We also consider a slightly weaker form of adaptive security denoted $\mathsf{IND\text{-}CPA}$*-security where attribute hiding property is not achieved. In the corresponding security game, denoted* $\textit{ind-cpa}$*,* $\widehat{\mathbf{x}}_1 = \widehat{\mathbf{x}}_2$ *that is, there is only one challenge attribute vector* $\widehat{\mathbf{x}}$*.*

3 Variant of Jutla-Roy Split-CRS NIZK Proof and IBE

In this section, we suggest a small modification to QA-NIZK proofs of Jutla and Roy [JR13] and describe an IBE derived from it. We denote the IBE as $\mathcal{JR}$-$\mathcal{IBE}$-$\mathcal{D}$, the 'd' signifying a sort of 'dual' of the original scheme. $\mathcal{JR}$-$\mathcal{IBE}$-$\mathcal{D}$ forms the basis of our IPE construction with short ciphertexts. Since the QA-NIZK construction only points a way to the IBE construction, we provide an informal description of the modification required without delving into details of the construction or proof. For definitions and more details related to QA-NIZK proofs we refer to [JR13].

We are mainly interested in NIZK proofs for languages that are linear subspaces of vectors of $\mathbb{G}_2$-elements. [JR13] actually considers vectors over $\mathbb{G}_1$. Since $\mathbb{G}_1$ has shorter representation compared to $\mathbb{G}_2$, we prefer the ciphertext components to live in $\mathbb{G}_1$ and hence reverse the roles of $\mathbb{G}_1$ and $\mathbb{G}_2$ in our presentation. A linear subspace language is parameterised by an $t \times m$ matrix $\mathbf{A}$ of $\mathbb{G}_2$-elements and defined as

$$L_{\mathbf{A}} = \{\mathbf{x}^T\mathbf{A} \mid \mathbf{x} \in \mathbb{Z}_p^t\}.$$

A NIZK proof system for this language is a collection of four algorithms $(\mathsf{K}_0, \mathsf{K}_1, \mathsf{P}, \mathsf{V})$ where K_0 generates the common parameters (group descriptions for a pairing), K_1 generates CRS_p and CRS_v, the prover and verifier CRS's respectively, P generates a proof given a witness $\mathbf{x}$ for a candidate $\vec{Q} \in L_{\mathbf{A}}$ and V verifies that the proof is valid. Quasi-adaptiveness refers to the CRS being allowed to depend on the parameter, ($\mathbf{A}$ in the above case). Three notions – completeness, soundness and zero-knowledge – formalise the security requirements of a NIZK proof system. [JR13] starts with an efficient construction for this language and then extends it to what they call the split-CRS QA-NIZK system. The languages supported by such systems are characterised as

$$L_{\mathbf{A},\vec{A}_1,\vec{A}_2} = \{\mathbf{x}^T \cdot [\mathbf{A}|\vec{A}_1 + \mathsf{ctag} \cdot \vec{A}_2] \mid \mathbf{x} \in \mathbb{Z}_p^t, \mathsf{ctag} \in \mathbb{Z}_p\},$$

with $\mathbf{A} \in \mathbb{G}_2^{t\times m}$, $\vec{A}_1, \vec{A}_2 \in \mathbb{G}_2^t$ are parameters defining the language. Writing $\mathbf{A}$ as $[\mathbf{A}_l|\mathbf{A}_r]$ with $\mathbf{A}_l \in \mathbb{G}_2^{t\times t}$ and $\mathbf{A}_r \in \mathbb{G}_2^{(m-t)\times t}$ and assuming that the number $(m-t)$ of equations in excess of the number of unknowns can be verified by just making additional randomised copies of the CRS [JR13], we only consider $\mathbf{A}_l$ in our descriptions. The algorithms of the split-CRS NIZK system are described below.

K_0: Generates the bilinear pairing parameters $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, P_1, P_2)$.

K_1**:** Generates CRS as

$$\mathsf{CRS}_{p,0} = \left[\mathbf{A}_l | \vec{A}_1\right] \begin{bmatrix} \mathbf{u}_1 \\ b^{-1} \end{bmatrix} \qquad \mathsf{CRS}_{p,1} = \left[\mathbf{A}_l | \vec{A}_2\right] \begin{bmatrix} \mathbf{u}_2 \\ b^{-1} \end{bmatrix}$$

$$\mathsf{CRS}_{v,0} = \begin{bmatrix} b\mathbf{u}_1 \\ 1 \\ -b \end{bmatrix} P_1 \qquad \mathsf{CRS}_{v,1} = \begin{bmatrix} b\mathbf{u}_2 \\ 0 \\ 0 \end{bmatrix} P_1,$$

where $\mathbf{u}_1, \mathbf{u}_2 \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p^t$ and $b \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p^{\times}$. Note that $\mathsf{CRS}_{v,0}, \mathsf{CRS}_{v,1} \in \mathbb{G}_1^{t+2}$.

P**:** Suppose the candidate is $\vec{Q} = \mathbf{x}^T \cdot [\mathbf{A}|\vec{A}_1 + \mathsf{ctag} \cdot \vec{A}_2]$. The proof is given by

$$\vec{R} = \mathbf{x}^T (\mathsf{CRS}_{p,0} + \mathsf{ctag} \cdot \mathsf{CRS}_{p,1}).$$

V**:** Given a proof $\vec{R}$ for a candidate $\vec{Q}$, the verifier checks whether

$$e\left([\vec{R} \mid \vec{Q}], \mathsf{CRS}_{v,0} + \mathsf{ctag} \cdot \mathsf{CRS}_{v,1}\right)$$

equals 1_T, the identity of $\mathbb{G}_T$ or not indicating validity of the proof or otherwise, respectively. Here the pairing function e evaluated on vectors is nothing but the product of the component-wise evaluations.

Our Modification. We are now ready to propose our tweak to this split-CRS NIZK system. Instead of combining the verifier CRS's during verification, consider providing only one verifier CRS defined as

$$\mathsf{CRS}_v = \mathsf{CRS}_{v,0} + \mathsf{ktag}\mathsf{CRS}_{v,1}$$

where $\mathsf{ktag} \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p$ is chosen in K_1. Verification is now done by testing whether

$$e\left([\vec{R} \mid \vec{Q}], \mathsf{CRS}_v\right)^{\frac{1}{(\mathsf{ctag}-\mathsf{ktag})}}$$

is 1_T only if $\mathsf{ctag} \neq \mathsf{ktag}$. Verification fails unconditionally if the two tags are equal. The modification weakens the quasi-adaptive soundness criterion since there is a probability that the verification algorithm fails. However, we make this modification only to make a transition to attribute-based encryption. Whether this NIZK system is actually useful for other purposes is beyond the scope of this work.

IBE. We now present the identity-based encryption scheme obtained from the above mentioned NIZK system.

$\mathsf{Setup}(\kappa)$**:** Let $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, F_1, F_2)$ be a Type-3 pairing ensemble generated based on the security parameter κ. Choose $P_1 \overset{\text{U}}{\longleftarrow} \mathbb{G}_1^{\times}$, $P_2 \overset{\text{U}}{\longleftarrow} \mathbb{G}_2^{\times}$, $b \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p^{\times}$, $\alpha_1, \alpha_2, u_1, u_2, v_1, v_2, w_1, w_2 \overset{\text{U}}{\longleftarrow} \mathbb{Z}_p$ and set $U_1 = (u_1 + bu_2)P_1$, $V_1 = (v_1 + bv_2)P_1$, $W_1 = (w_1 + bw_2)P_1$, $g_T = e(P_1, P_2)^{\alpha_1 + b\alpha_2}$. The parameters are given by

$\mathcal{PP} : (P_1, bP_1, U_1, V_1, W_1, g_T)$
$\mathcal{MSK} : (P_2, \alpha_1, \alpha_2, u_1, u_2, v_1, v_2, w_1, w_2)$

$\mathsf{Encrypt}(\mathcal{PP}, m, \mathsf{id})$**:** The ciphertext is given by $\mathcal{C} = (C_0, C_1, C_2, C_3, \mathsf{ctag})$ where

$\mathsf{ctag}, s \xleftarrow{\text{U}} \mathbb{Z}_p,$
$C_0 = m \cdot (g_T)^s,$
$C_1 = sP_1,\ C_2 = sbP_1,\ C_3 = s(U_1 + \mathsf{id}V_1 + \mathsf{ctag}W_1).$

$\mathsf{KeyGen}(\mathcal{MSK}, \mathsf{id})$ Compute the secret key $\mathcal{SK}_{\mathsf{id}} = (K_1, K_2, K_3, K_4, K_5, \mathsf{ktag})$ as follows.

$r, \mathsf{ktag} \xleftarrow{\text{U}} \mathbb{Z}_p,$
$K_1 = rP_2,\ K_2 = (\alpha_1 + rw_1)\,P_2,\ K_3 = (\alpha_2 + rw_2)\,P_2$
$K_4 = r(u_1 + \mathsf{id}v_1 + \mathsf{ktag}w_1)P_2,\ K_5 = r(u_2 + \mathsf{id}v_2 + \mathsf{ktag}w_2)P_2.$

$\mathsf{Decrypt}(\mathcal{C}, \mathcal{SK}_{\mathsf{id}})$: If $\mathsf{ctag} = \mathsf{ktag}$, return $\perp$. Otherwise compute

$$A = \left(\frac{e(C_3, K_1)}{e(C_1, K_4)e(C_2, K_5)}\right)^{\frac{1}{\mathsf{ctag}-\mathsf{ktag}}}$$

and recover the message as

$$m = \frac{C_0 \cdot A}{e(C_1, K_2)e(C_2, K_3)}.$$

The message m can be recovered in a single step involving 3 pairing operations.

Decryption involves the two-equation revocation technique of Sahai and Waters [LSW08] that was also used in Waters IBE [Wat09]. The scheme is adaptively secure under the SXDH assumption. Since $\mathcal{JR}$-$\mathcal{IBE}$-$\mathcal{D}$ is a special case of $\mathcal{IPE}_1$, its security is implied by that of $\mathcal{IPE}_1$. Hence we omit the proof.

4 IPE with Short Ciphertexts

In this section, we define our first IPE construction $\mathcal{IPE}_1$ with constant-size ciphertexts and show that it is adaptively secure. As mentioned earlier, we use the n-equation revocation technique of Attrapadung and Libert [AL10] to extend $\mathcal{JR}$-$\mathcal{IBE}$-$\mathcal{D}$ to support inner product encryption. Below is the description of the algorithms of $\mathcal{IPE}_1 = (\mathcal{IPE}_1.\mathsf{Setup}, \mathcal{IPE}_1.\mathsf{Encrypt}, \mathcal{IPE}_1.\mathsf{KeyGen}, \mathcal{IPE}_1.\mathsf{Decrypt})$.

$\mathcal{IPE}_1.\mathsf{Setup}(\kappa, n)$**:** Generate a Type-3 pairing $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, F_1, F_2)$ based on the security parameter κ. Choose $P_1 \xleftarrow{\text{U}} \mathbb{G}_1^\times$, $P_2 \xleftarrow{\text{U}} \mathbb{G}_2^\times$, $b \xleftarrow{\text{U}} \mathbb{Z}_p^\times$, $\alpha_1, \alpha_2, w_1, w_2 \xleftarrow{\text{U}} \mathbb{Z}_p$, $\mathbf{u}_1 = (u_{1,1}, \ldots, u_{1,n}), \mathbf{u}_2 = (u_{2,1}, \ldots, u_{2,n}) \xleftarrow{\text{U}} \mathbb{Z}_p^n$ and set $\mathbf{u} = (\mathbf{u}_1 + b\mathbf{u}_2)P_1$, $w = (w_1 + bw_2)$, $g_T = e(P_1, P_2)^{\alpha_1 + b\alpha_2}$. The parameters are given by

$\mathcal{PP} : (P_1, bP_1, \mathbf{u}P_1, wP_1, g_T)$
$\mathcal{MSK} : (P_2, \alpha_1, \alpha_2, \mathbf{u}_1, \mathbf{u}_2, w_1, w_2)$

$\mathcal{IPE}_1.\mathsf{Encrypt}(\mathcal{PP}, m, \mathbf{x} = (x_1, \ldots, x_n))$**:** Components of the ciphertext are computed as follows.

$\mathsf{ctag}, s \xleftarrow{\text{U}} \mathbb{Z}_p,$
$C_0 = m \cdot (g_T)^s,$
$C_1 = sP_1,\ C_2 = sbP_1,\ C_3 = s(\langle \mathbf{x}, \mathbf{u} \rangle + \mathsf{ctag} \cdot w)P_1.$

Note that C_3 can be computed from $\mathbf{u}P_1$, wP_1 and ctag using $n+1$ scalar multiplications. The ciphertext is given by $\mathcal{C} = (\mathbf{x}, C_0, C_1, C_2, C_3, \mathsf{ctag})$.

$\mathcal{IPE}_1.\mathsf{KeyGen}(\mathcal{MSK}, \mathbf{y} = (y_1, \ldots, y_n))$**:** The secret key for $\mathbf{y}$ is given by $\mathcal{SK}_{\mathbf{y}} = (K_1, K_2, K_3, (K_{4,i}, K_{5,i}, \mathsf{ktag}_i)_{i=2}^n)$ where

$r, (\mathsf{ktag}_i)_{i=2}^n \xleftarrow{\text{U}} \mathbb{Z}_p,$
$K_1 = rP_2,\ K_2 = (\alpha_1 + rw_1)P_2,\ K_3 = (\alpha_2 + rw_2)P_2,$
For $i = 2, \ldots, n,$
$K_{4,i} = r(-u_{1,1}\frac{y_i}{y_1} + u_{1,i} + \mathsf{ktag}_i w_1)P_2,$
$K_{5,i} = r(-u_{2,1}\frac{y_i}{y_1} + u_{2,i} + \mathsf{ktag}_i w_2)P_2.$

$\mathcal{IPE}_1.\mathsf{Decrypt}(\mathcal{C}, \mathcal{SK}_{\mathbf{y}})$**:** Compute $\mathsf{ktag} = \sum_{i=2}^n x_i \mathsf{ktag}_i$. If $\mathsf{ctag} = \mathsf{ktag}$, return $\perp$. Otherwise let

$$A = \left(e(C_3, K_1) e(C_1, \sum_{i=2}^n x_i K_{4,i})^{-1} e(C_2, \sum_{i=2}^n x_i K_5)^{-1} \right)^{\frac{1}{\mathsf{ctag} - \mathsf{ktag}}}.$$

Recover the message as $m = \frac{C_0 \cdot A}{e(C_1, K_2) e(C_2, K_3)}$. As in the IBE, decryption can be done in a single step involving 3 pairings.

Correctness: Let $\mathcal{C} \longleftarrow \mathcal{IPE}_1.\mathsf{Encrypt}(\mathcal{PP}, m, \mathbf{x} = (x_1, \ldots, x_n); s)$ where $\mathcal{C} = (\mathbf{x}, C_0, C_1, C_2, C_3, \mathsf{ctag})$ and let $\mathcal{SK}_{\mathbf{y}} \longleftarrow \mathcal{IPE}_1.\mathsf{KeyGen}(\mathcal{MSK}, \mathbf{y} = (y_1, \ldots, y_n); r)$ with $\mathcal{SK}_{\mathbf{y}} = (K_1, K_2, K_3, (K_{4,i}, K_{5,i}, \mathsf{ktag}_i)_{i=2}^n)$. Suppose $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ and $\mathsf{ktag} = \sum_{i=2}^n x_i \mathsf{ktag}_i \neq \mathsf{ctag}$. First, we look at the computation of A. We have

$$\begin{aligned}
\sum_{i=2}^n x_i K_{4,i} &= \sum_{i=2}^n x_i r(-u_{1,1}\frac{y_i}{y_1} + u_{1,i} + \mathsf{ktag}_i w_1)P_2 \\
&= r\left(-\frac{u_{1,1}}{y_1} \sum_{i=2}^n x_i y_i + \sum_{i=2}^n x_i u_{1,i} + w_1 \sum_{i=2}^n x_i \mathsf{ktag}_i \right) P_2 \\
&= r\left(-\frac{u_{1,1}}{y_1} (\langle \mathbf{x}, \mathbf{y} \rangle - x_1 y_1) + \langle \mathbf{x}, \mathbf{u}_1 \rangle - x_1 u_{1,1} + \mathsf{ktag} \cdot w_1 \right) P_2 \\
&= r\left(\langle \mathbf{x}, \mathbf{u}_1 \rangle + \mathsf{ktag} \cdot w_1 \right) P_2.
\end{aligned}$$

Similarly, $\sum_{i=2}^n x_i K_{5,i} = r\left(\langle \mathbf{x}, \mathbf{u}_2 \rangle + \mathsf{ktag} \cdot w_1 \right) P_2$. Combining the two, we get

$$e(C_1, \sum_{i=2}^n x_i K_{4,i}) e(C_2, \sum_{i=2}^n x_i K_5) = e(P_1, P_2)^{rs(\langle \mathbf{x}, \mathbf{u} \rangle + \mathsf{ktag} \cdot w)}$$

implying that

$$A = \left(e(C_3, K_1) e(C_1, \sum_{i=2}^{n} x_i K_{4,i})^{-1} e(C_2, \sum_{i=2}^{n} x_i K_5)^{-1} \right)^{\frac{1}{\mathsf{ctag}-\mathsf{ktag}}} = e(P_1, P_2)^{rsw}.$$

The second stage of decryption recovers the message as shown below.

$$\begin{aligned} \frac{C_0 \cdot A}{e(C_1, K_2) e(C_2, K_3)} &= \frac{m \cdot g_T^s \cdot A}{e(sP_1, (\alpha_1 + rw_1)P_2) e(sbP_1, (\alpha_2 + rw_2)P_2)} \\ &= \frac{m \cdot e(P_1, P_2)^{(\alpha_1 + b\alpha_2)s} \cdot e(P_1, P_2)^{rsw}}{e(P_1, P_2)^{(\alpha_1 + b\alpha_2)s} e(P_1, P_2)^{rsw}} \\ &= m \end{aligned}$$

Before proving security, we describe algorithms that generate the necessary semi-functional objects for a dual system proof. These are required only in the proof.

$\mathcal{IPE}_1$.SFEncrypt$(\mathcal{PP}, \mathcal{MSK}, m, \mathbf{x})$**:** Generate $(\mathcal{C}' = (\mathbf{x}, C_0, C_1, C_2, C_3, \mathsf{ctag})) \xleftarrow{\text{R}}$ $\mathcal{IPE}_1$.Encrypt$(\mathcal{PP}, m, \mathbf{x})$. Choose $\mu \xleftarrow{\text{U}} \mathbb{Z}_p$ and generate the semi-functional ciphertext components as follows.

$$\begin{aligned} &C_0 \longleftarrow C_0 \cdot e(P_1, P_2)^{\mu\alpha_1}, \\ &C_1 \longleftarrow C_1 + \mu P_1,\ C_3 \longleftarrow C_3 + \mu(\langle \mathbf{x}, \mathbf{u}_1 \rangle + \mathsf{ctag} \cdot w_1). \end{aligned}$$

Return $\mathcal{C} = (\mathbf{x}, C_0, C_1, C_2, C_3, \mathsf{ctag})$ as the resulting semi-functional ciphertext.

$\mathcal{IPE}_1$.SFKeyGen$(\mathcal{PP}, \mathcal{MSK}, \mathbf{y})$**:** Let $\mathcal{SK}'_{\mathbf{y}} = (K_1, K_2, K_3, (K_{4,i}, K_{5,i}, \mathsf{ktag}_i)_{i=2}^{n})$ be obtained by running $\mathcal{IPE}_1$.KeyGen$(\mathcal{MSK}, \mathbf{y})$. Pick $\gamma \xleftarrow{\text{U}} \mathbb{Z}_p$ and modify the components of $\mathcal{SK}'_{\mathbf{y}}$ as follows:

$$K_2 \longleftarrow K_2 + \gamma P_2,\ K_3 \longleftarrow K_3 - \tfrac{\gamma}{b} P_2.$$

The semi-functional key given by $\mathcal{SK}'_{\mathbf{y}} = (K_1, K_2, K_3, (K_{4,i}, K_{5,i}, \mathsf{ktag}_i)_{i=2}^{n})$ is returned as output.

For a given pair of ciphertext and key satisfying $(\mathsf{ktag} = \sum_{i=2}^{n} x_i \mathsf{ktag}_i) \neq \mathsf{ctag}$ and $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, decryption fails only when both are semi-functional since the message will be blinded by $e(P_1, P_2)^{\mu\gamma}$. It is easy to see that the rest of the semi-functional components get canceled.

We now prove that scheme $\mathcal{IPE}_1$ is adaptively secure, formalised in the theorem below.

Theorem 1. *Scheme $\mathcal{IPE}_1$ is (q, ε, t)-IND-CPA-secure if the $(\varepsilon_{\text{DDH1}}, t_1)$-DDH1 and $(\varepsilon_{\text{DDH2}}, t_2)$-DDH2 assumptions hold in the underlying pairing description $\mathcal{G}$ where $\varepsilon \leq \varepsilon_{\text{DDH1}} + q \cdot \varepsilon_{\text{DDH2}} + (1/p)$ and $t = \max(t_1, t_2) - O(q\rho)$, ρ being the maximum cost of scalar multiplication in either $\mathbb{G}_1$ or $\mathbb{G}_2$.*

Proof Sketch. Let G_0 denote the real security game $\mathsf{ind\text{-}cpa}$ (defined in Sect. 2.3). The proof proceeds though a sequence of games where we gradually change the distribution of the keys and challenge ciphertext provided to the adversary. At the end is the game where the attacker receives semi-functional encryption of a random message. We first change the ciphertext to semi-functional form and then the q keys provided as answers to the q queries to semi-functional form. There are essentially three main parts in the reduction.

Distinguishing normal and semi-functional ciphertexts: We show that an attacker's ability to distinguish between normal and semi-functional ciphertexts can be leveraged to solve the DDH1 problem. This is clear from the definition of semi-functional ciphertexts. P_1, bP_1 and sbP_1 come from the instance and are sufficient to simulate the correct environment. The DDH1 challenge is embedded in C_1 which is either normal or semi-functional according as the instance is real or random. Since no encoding of b is known in $\mathbb{G}_2$, the simulator itself cannot create a semi-functional key and detect the type of the challenge ciphertext.

Detecting whether k-th key is normal or semi-functional: This is the most crucial stage of the security reduction. Denote by $\mathbf{y}_1, \ldots, \mathbf{y}_q$ the queries made by the attacker. The first $k-1$ keys returned are semi-functional and the last $q-k-1$ keys are normal. The simulator is designed in a way that it can create both normal and semi-functional keys. The DDH2 challenge is embedded in the k-th key and particularly in component K_2. However, for the k-th key the simulator can only create a semi-functional ciphertext with $\mathsf{ctag} = \sum_{i=2}^{n} x_i \mathsf{ktag}_i$. This ensures that the simulator itself cannot detect the type of k-th key and trivially solve DDH2. Furthermore, the tags in the ciphertext and keys need to be uniformly and independently distributed in the attacker's view. This is achieved by setting them as

$$\begin{pmatrix} \widehat{\mathsf{ctag}} \\ \mathsf{ktag}_2 \\ \vdots \\ \mathsf{ktag}_n \end{pmatrix} = \begin{pmatrix} -\widehat{x}_1 & -\widehat{x}_2 & -\widehat{x}_3 & \cdots & -\widehat{x}_n \\ y_2/y_1 & -1 & 0 & \cdots & 0 \\ y_3/y_1 & 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y_n/y_1 & 0 & 0 & \cdots & -1 \end{pmatrix} \begin{pmatrix} v_{2,1} \\ v_{2,2} \\ \vdots \\ v_{2,n} \end{pmatrix}$$

where $\widehat{\mathsf{ctag}}$ is the tag associated with the challenge ciphertext for the challenge vector $\widehat{\mathbf{x}} = (\widehat{x}_1, \ldots, \widehat{x}_n)$ and $\mathsf{ktag}_2, \ldots, \mathsf{ktag}_n$ are the tags associated with the secret key for $\mathbf{y}_k$. The matrix has determinant $(-1)^n \langle \widehat{\mathbf{x}}, \mathbf{y}_k \rangle / y_1$ which is non-zero because all of $\mathscr{A}$'s queries are such that $\langle \widehat{\mathbf{x}}, \mathbf{y}_k \rangle \neq 0$. (Here y_1 is the first coordinate of $\mathbf{y}_k$). Hence all we need to do is choose $\mathbf{v}_2 = (v_{2,1}, \ldots, v_{2,n})$ uniformly from $\mathbb{Z}_p^n$ and also hide $\mathbf{v}_2$ information theoretically from the attacker. $\mathbf{v}_2$ is in fact embedded in the master secret key (and as a result in the public parameters) but masked by other additive terms. The argument repeated q times for each query gives a degradation of q in DDH2.

Distinguishing the real message from a random one: The last important step is an information theoretic argument to show that the message encrypted is random that is, the bit β is statistically hidden form the attacker. This is done by changing the setup and semi-functional key generation algorithms in such a way that all information provided to the attacker are independent of α_1. The only component that depends on α_1 is C_0 of the challenge ciphertext where the message has a blinding factor of $e(P_1, P_2)^{\mu\alpha_1}$. Since all other information is independent of α_1, $m_\beta \cdot e(P_1, P_2)^{\mu\alpha_1}$ is uniformly distributed in $\mathbb{G}_T$ and thus provides no hint to about β unless $\mu = 0$ which happens with probability $1/p$.

Refer to the full version [Ram16] for details of the proof.

5 Weakly Attribute-Hiding IPE

In this section, we present our second IPE construction $\mathcal{IPE}_2$ for inner products over $\mathbb{Z}_p^n$. Unlike $\mathcal{IPE}_1$, this construction is based on $\mathcal{JR}$-$\mathcal{IBE}$. While the n-equation revocation technique was used in [AL10] to obtain constant-size ciphertexts forgoing attribute-hiding, we use it here to anonymise ciphertexts by incorporating the technique into the encryption algorithm. We split the ciphertext component of $\mathcal{JR}$-$\mathcal{IBE}$ containing the identity hash into $n-1$ components corresponding to the entries of the attribute vector $\mathbf{x}$. For decryption, the relation $R(\mathbf{x}, \mathbf{y})$ can be verified by combining the ciphertext components using the secret vector $\mathbf{y}$ without knowing $\mathbf{x}$. Described below are the algorithms of $\mathcal{IPE}_2 = (\mathcal{IPE}_2.\mathsf{Setup}, \mathcal{IPE}_2.\mathsf{Encrypt}, \mathcal{IPE}_2.\mathsf{KeyGen}, \mathcal{IPE}_2.\mathsf{Decrypt})$.

$\mathcal{IPE}_2.\mathsf{Setup}(\kappa, n)$: Generate a Type-3 pairing $\mathcal{G} = (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, F_1, F_2)$ based on the security parameter κ. Choose $P_1 \xleftarrow{\text{U}} \mathbb{G}_1^\times$, $P_2 \xleftarrow{\text{U}} \mathbb{G}_2^\times$, $b \xleftarrow{\text{U}} \mathbb{Z}_p^\times$, $\alpha_1, \alpha_2, w_1, w_2 \xleftarrow{\text{U}} \mathbb{Z}_p$, $\mathbf{u}_1, \mathbf{u}_2 \xleftarrow{\text{U}} \mathbb{Z}_p^n$ and set $\mathbf{u} = \mathbf{u}_1 + b\mathbf{u}_2$, $w = w_1 + bw_2$ and $g_T = e(P_1, P_2)^{\alpha_1 + b\alpha_2}$. The parameters are given by

$$\mathcal{PP} : (P_1, bP_1, \mathbf{u}P_1, wP_1, g_T)$$
$$\mathcal{MSK} : (P_2, \alpha_1, \alpha_2, \mathbf{u}_1, \mathbf{u}_2, w_1, w_2)$$

$\mathcal{IPE}_2.\mathsf{Encrypt}(\mathcal{PP}, m, \mathbf{x} = (x_1, \ldots, x_n))$: The ciphertext is given by the tuple $\mathcal{C} = (C_0, C_1, C_2, (C_{3,i}, \mathsf{ctag}_i)_{i=2}^n)$ where

$$(\mathsf{ctag}_i)_{i=2}^n, s \xleftarrow{\text{U}} \mathbb{Z}_p,$$
$$C_0 = m \cdot (g_T)^s,$$
$$C_1 = sP_1,\ C_2 = sbP_1,$$
$$C_{3,i} = s\left(-\frac{x_i}{x_1}u_1 + u_i + \mathsf{ctag}_i w\right)P_1 \text{ for } i = 2, \ldots, n.$$

Since $(u_i P_1)_{i\in[1,n]}$ and wP_1 are provided in $\mathcal{PP}$, each $C_{3,i}$ can be computed using 3 scalar multiplications.

$\mathcal{IPE}_2.\mathsf{KeyGen}(\mathcal{MSK}, \mathbf{y} = (y_1, \ldots, y_n))$: Secret key $\mathcal{SK}_\mathbf{y} = (K_1, K_2, K_3, K_4, K_5)$ is computed as follows.

$$r \xleftarrow{\text{U}} \mathbb{Z}_p,$$
$$K_1 = rP_2,\ K_2 = (\alpha_1 + r\langle \mathbf{y}, \mathbf{u}_1\rangle)P_2,\ K_3 = (\alpha_2 + r\langle \mathbf{y}, \mathbf{u}_2\rangle)P_2$$
$$K_4 = rw_1P_2,\ K_5 = rw_2P_2.$$

$\mathcal{IPE}_2$.$\mathsf{Decrypt}(\mathcal{C}, \mathcal{SK}_{\mathbf{y}}, \mathbf{y})$**:** Compute $\mathsf{ctag} = \sum_{i=2}^{n} y_i \mathsf{ctag}_i$. Recover the message as follows.

$$m = \frac{C_0 \cdot e(\sum_{i=2}^{n} y_i C_{3,i}, K_1)}{e(C_1, K_2 + \mathsf{ctag} K_4) e(C_2, K_3 + \mathsf{ctag} K_5)}.$$

Correctness. Let $\mathcal{C} \xleftarrow{\text{R}} \mathcal{IPE}_2.\mathsf{Encrypt}(\mathcal{PP}, m, \mathbf{x} = (x_1, \ldots, x_n); s)$ and let $\mathcal{SK}_{\mathbf{y}} \xleftarrow{\text{R}} \mathcal{IPE}_2.\mathsf{KeyGen}(\mathcal{MSK}, \mathbf{y} = (y_1, \ldots, y_n); r)$ where $\mathcal{C}$, $\mathcal{SK}_{\mathbf{y}}$ are given by $(C_0, C_1, C_2, (C_{3,i}, \mathsf{ctag}_i)_{i=2}^{n})$, $\mathcal{SK}_{\mathbf{y}} = (K_1, K_2, K_3, K_4, K_5)$ respectively. Suppose $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ and $\mathsf{ctag} = \sum_{i=2}^{n} y_i \mathsf{ctag}_i$. Let $A_1 = e(\sum_{i=2}^{n} y_i C_{3,i}, K_1)$ and $A_2 = e(C_1, K_2 + \mathsf{ctag} K_4) e(C_2, K_3 + \mathsf{ctag} K_5)$. Decryption is correct if $A_2/A_1 = (g_T)^s$. We have

$$\begin{aligned} A_1 &= e\left(\sum_{i=2}^{n} y_i C_{3,i}, K_1\right) \\ &= e\left(\sum_{i=2}^{n} y_i s \left(-\frac{x_i u_1}{x_1} + u_i + \mathsf{ctag}_i w\right) P_1, r P_2\right) \\ &= e\left(\left(-(\langle \mathbf{y}, \mathbf{x} \rangle - x_1 y_1)\frac{u_1}{x_1} + \langle \mathbf{y}, \mathbf{u} \rangle - y_1 u_1 + \mathsf{ctag} \cdot w\right) P_1, P_2\right)^{rs} \\ &= e\left(P_1, P_2\right)^{rs(\langle \mathbf{y}, \mathbf{u} \rangle + \mathsf{ctag} \cdot w)}, \end{aligned}$$

and

$$\begin{aligned} A_2 &= e(C_1, K_2 + \mathsf{ctag} K_4) e(C_2, K_3 + \mathsf{ctag} K_5) \\ &= e(sP_1, (\alpha_1 + r\langle \mathbf{y}, \mathbf{u}_1 \rangle) P_2 + \mathsf{ctag} \cdot r w_1 P_2) \\ &\qquad \cdot e(sbP_1 \left(\alpha_2 + r\langle \mathbf{y}, \mathbf{u}_2 \rangle\right) P_2 + \mathsf{ctag} \cdot r w_2 P_2) \\ &= e\left(P_1, (\alpha_1 + b\alpha_2) P_2\right)^s e\left(P_1, r(\langle \mathbf{y}, \mathbf{u}_1 \rangle + b\langle \mathbf{y}, \mathbf{u}_2 \rangle + \mathsf{ctag}(w_1 + b w_2)) P_2\right)^s \\ &= (g_T)^s \cdot e\left(P_1, (\langle \mathbf{y}, \mathbf{u}_1 + b\mathbf{u}_2 \rangle + \mathsf{ctag} \cdot w) P_2\right)^{rs} \\ &= (g_T)^s \cdot e\left(P_1, P_2\right)^{rs(\langle \mathbf{y}, \mathbf{u} \rangle + \mathsf{ctag} \cdot w)} \end{aligned}$$

thus implying that $A_2/A_1 = (g_T)^s$, as desired.

Security. The theorem below summarises the security guarantee we obtain for $\mathcal{IPE}_2$.

Theorem 2. *Scheme* $\mathcal{IPE}_2$ *is* (q, ε, t)-IND-WAH-CPA-*secure if the* $(\varepsilon_{\text{DDH1}}, t_1)$-DDH1 *and* $(\varepsilon_{\text{DDH2}}, t_2)$-DDH2 *assumptions hold in the underlying pairing description* $\mathcal{G}$ *where* $\varepsilon \le \varepsilon_{\text{DDH1}} + q \cdot \varepsilon_{\text{DDH2}} + (1/p)$ *and* $t = \max(t_1, t_2) - O(q\rho)$, ρ *being the maximum cost of scalar multiplication in either* $\mathbb{G}_1$ *or* $\mathbb{G}_2$.

The proof is more or less similar to the proof of Theorem 1 except for the information theoretic argument in the last step. In addition to showing that the blinding factor on the message is uniformly random in the attacker's view, we also need to prove that the attribute vector is hidden from the adversary. The solution is to simulate the key extraction queries in such a way that all information the attacker sees is independent of $\mathbf{u}_1$. Observe that $\mathbf{u}_1$ is part of the master secret and would also be used to define the semi-functional components for $C_{3,i}$. With all keys and parameters being independent of $\mathbf{u}_1$, one can argue that $C_{3,i}$ components are uniform and independent elements of $\mathbb{G}_1$ thus providing no hint about which attribute vector the challenge ciphertext is encrypted to. (This makes sense as the only ciphertext components determined by the attribute vector are $C_{3,i}$ for $i = 2, \ldots, n$). A detailed proof is provided in the full version [Ram16].

Acknowledgements. I would like to thank Benoit Libert and Palash Sarkar for helpful discussions as well as the reviewers of ACNS'16 for their valuable comments. This research was funded by the "Programme Avenir Lyon Saint-Etienne de l'Universite de Lyon" in the framework of the programme "Investissements d'Avenir" (ANR-11-IDEX-0007).

References

[AL10] Attrapadung, N., Libert, B.: Functional encryption for inner product: achieving constant-size ciphertexts with adaptive security or support for negation. In: Nguyen, P.Q., Pointcheval, D. (eds.) PKC 2010. LNCS, vol. 6056, pp. 384–402. Springer, Heidelberg (2010)

[Att14] Attrapadung, N.: Dual system encryption via doubly selective security: framework, fully secure functional encryption for regular languages, and more. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 557–577. Springer, Heidelberg (2014)

[Att15] Attrapadung, N.: Dual system encryption framework in prime-order groups. IACR Cryptology ePrint Archive 2015:390 (2015)

[BKP14] Blazy, O., Kiltz, E., Pan, J.: (Hierarchical) identity-based encryption from affine message authentication. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 408–425. Springer, Heidelberg (2014)

[Boy13] Boyen, X.: Attribute-based functional encryption on lattices. In: Sahai, A. (ed.) TCC 2013. LNCS, vol. 7785, pp. 122–142. Springer, Heidelberg (2013)

[BSW07] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy, pp. 321–334. IEEE Computer Society (2007)

[CG13] Canetti, R., Garay, J.A. (eds.): CRYPTO 2013, Part II. LNCS, vol. 8043. Springer, Heidelberg (2013)

[CGW15] Chen, J., Gay, R., Wee, H.: Improved dual system ABE in prime-order groups via predicate encodings. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9057, pp. 595–624. Springer, Heidelberg (2015)

[CW13] Chen, J., Wee, H.: Fully, (almost) tightly secure IBE and dual system groups. In: Canetti, Garay (eds.) [CG13], pp. 435–460. Full version available as IACR Technical Report, 2013/803. http://eprint.iacr.org/2013/803

[GGH+13] Garg, S., Gentry, C., Halevi, S., Sahai, A., Waters, B.: Attribute-based encryption for circuits from multilinear maps. In: Canetti, Garay (eds.) [CG13], pp. 479–499

[GPSW06] Goyal, V., Pandey, O., Sahai, A., Waters, B.: Attribute-based encryption for fine-grained access control of encrypted data. In: Juels, A., Wright, R.N., De Capitani di Vimercati, S. (eds.) ACM Conference on Computer and Communications Security, pp. 89–98. ACM (2006)

[GVW13] Gorbunov, S., Vaikuntanathan, V., Wee, H.: Attribute-based encryption for circuits. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) Symposium on Theory of Computing Conference, STOC 2013, Palo Alto, CA, USA, 1–4 June 2013, pp. 545–554. ACM (2013)

[GW09] Gentry, C., Waters, B.: Adaptive security in broadcast encryption systems (with short ciphertexts). In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 171–188. Springer, Heidelberg (2009)

[JR13] Jutla, C.S., Roy, A.: Shorter quasi-adaptive NIZK proofs for linear subspaces. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 1–20. Springer, Heidelberg (2013)

[JR15] Jutla, C.S., Roy, A.: Dual-system simulation-soundness with applications to UC-PAKE and more. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 628–653. Springer, Heidelberg (2015). doi: 10.1007/978-3-662-48797-6_26

[KSW08] Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 146–162. Springer, Heidelberg (2008)

[LSW08] Lewko, A.B., Sahai, A., Waters, B.: Revocation systems with very small private keys. IACR Cryptology ePrint Archive 2008:309 (2008)

[LW12] Lewko, A., Waters, B.: New proof methods for attribute-based encryption: achieving full security through selective techniques. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 180–198. Springer, Heidelberg (2012)

[OSW07] Ostrovsky, R., Sahai, A., Waters, B.: Attribute-based encryption with non-monotonic access structures. In: Ning, P., De Capitani di Vimercati, S., Syverson, P.F. (eds.) ACM Conference on Computer and Communications Security, pp. 195–203. ACM (2007)

[OT08] Okamoto, T., Takashima, K.: Homomorphic encryption and signatures from vector decomposition. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 57–74. Springer, Heidelberg (2008)

[OT09] Okamoto, T., Takashima, K.: Hierarchical predicate encryption for inner-products. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 214–231. Springer, Heidelberg (2009)

[OT10] Okamoto, T., Takashima, K.: Fully secure functional encryption with general relations from the decisional linear assumption. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 191–208. Springer, Heidelberg (2010)

[OT11] Okamoto, T., Takashima, K.: Achieving short ciphertexts or short secret-keys for adaptively secure general inner-product encryption. In: Lin, D., Tsudik, G., Wang, X. (eds.) CANS 2011. LNCS, vol. 7092, pp. 138–159. Springer, Heidelberg (2011)

[Ram16] Ramanna, S.C.: More efficient constructions for inner-product encryption. Cryptology ePrint Archive, Report 2016/356 (2016). http://eprint.iacr.org/

[RS14a] Ramanna, S.C., Sarkar, P.: Efficient adaptively secure IBBE from standard assumptions. IACR Cryptology ePrint Archive 2014:380 (2014)

[RS14b] Ramanna, S.C., Sarkar, P.: Efficient (anonymous) compact HIBE from standard assumptions. In: Chow, S.S.M., Liu, J.K., Hui, L.C.K., Yiu, S.M. (eds.) ProvSec 2014. LNCS, vol. 8782, pp. 243–258. Springer, Heidelberg (2014)

[SW05] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 457–473. Springer, Heidelberg (2005)

[Wat09] Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)

[Wat11] Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011)

[Wee14] Wee, H.: Dual system encryption via predicate encodings. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 616–637. Springer, Heidelberg (2014)