Disclaimer

Statement for open documents

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780108. Any dissemination of results here presented reflects only the consortium view.

D4.4 Annual Report on Functional Encryption Schemes for Richer Functionalities Y1

Document Identification			
Status	Final	**Due Date**	31/12/2018
Version	1.0	**Submission Date**	18/12/2018

Related WP	WP4	**Document Reference**	D4.4
Related Deliverable(s)	D4.1	**Dissemination Level(*)**	PU
Lead Participant	UEDIN	**Lead Author**	Hendrik Waldner
Contributors	ENS, UEDIN	**Reviewers**	Michel Abdalla (ENS) Marco Lewandowsky (FUAS)

Keywords:
Functional Encryption Schemes, Attribute-Based Encryption, Inner-Product Predicate Encryption, Video Surveillance

This document is issued within the framework and for the purpose of the FENTEC project. This project has received funding from the European Union's Horizon2020 under Grant Agreement No. 780108. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Document Information

List of Contributors	
Name	Partner
Michel Abdalla	ENS
Hendrik Waldner	UEDIN

Document History			
Version	Date	Change editors	Changes
0.1	22/11/2018	Hendrik Waldner (UEDIN)	ToC
0.2	13/12/2018	Hendrik Waldner (UEDIN)	Version for reviewing
0.3	14/12/2018	Hendrik Waldner (UEDIN)	Addressed reviewers comments
0.4	17/12/2018	Michel Abdalla (ENS)	Revised summary, introduction, and conclusion
1	18/12/2018	Hendrik Waldner (UEDIN)	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable Leader	Hendrik Waldner (ENS)	18/12/2018
Technical Manager	Michel Abdalla (ENS)	18/12/2018
Quality Manager	Diego Esteban (ATOS)	18/12/2018
Project Coordinator	Francisco Gala (ATOS)	18/12/2018

(*) Dissemination level.-PU: Public, fully open, e.g. web; CO: Confidential, restricted under conditions set out in Model Grant Agreement; CI: Classified, Int = Internal Working Document, information as referred to in Commission Decision 2001/844/EC.

Table of Contents

List of Acronyms

Acronym	Description
ABE	Attribute Based Encryption
CP-ABE	Ciphertext Policy Attribute Based Encryption
DDH	Decisional Diffie-Helmman
DLIN	Decisional LINear
FE	Functional Encryption
IPPE	Inner Product Predicate Encryption
k-LIN	k-LINear Assumption
KP-ABE	Key Policy Attribute Based Encryption
LWE	Learning With Errors
MSP	Monotone Span Program
PE	Predicate Encryption
PKE	Public Key Encryption
PPT	Probabilistic Polynomial Time
PTA	Polynomial-Time Adversary
XDLIN	eXternal Decisional LINear

Executive Summary

The concept of functional encryption (FE) [3, 16] is a generalization of standard encryption, which allows users to delegate to third parties the computation of certain classes of functions of the encrypted data by generating specific secret keys for these functions. Examples of FE schemes include attribute-based encryption (ABE) [17], inner-product predicate encryption (IPPE) [11], and functional encryption for all polynomial-size circuits [8]. In ABE, the encryptor is able to dynamically choose the set of people who will be authorized to decrypt a given ciphertext, by defining attributes and corresponding access policies. The secret keys can be associated with the attributes and the ciphertext with the policy or the other way around. In IPPE, ciphertexts and secret keys are associated with vectors and the decryption procedure only succeeds when the inner-product between these two vectors is equal to zero.

Among the above-mentioned examples of FE schemes, the latter one in [8], which relies on the powerful notion of indistinguishability obfuscation, is the primitive that provides the highest functionality as it implies all of the previous ones. Unfortunately, it is also impractical, making it interesting only from a theoretical point of view. Hence, one of the main goals of WP4 is to find a reasonable trade-off between efficiency and expressiveness. More precisely, our goal is to design schemes that cover reasonably expressive functionalities while still being efficient. In this deliverable, we describe our progress towards this goal.

More specifically, this report describes two contributions made in the context of FENTEC. First, we describe the unbounded attribute-based encryption scheme proposed by Chen et al. [5] with constant-size public parameters under static assumptions in bilinear groups. This scheme defines the current state of the art in the area of unbounded attribute-based encryption. Second, we describe the inner-product predicate encryption schemes introduced by Chen et al. [6]. The proposed schemes achieve adaptive security and full attribute-hiding in the prime-order bilinear group setting and improve current results by Okamoto et al. [15].

1 Introduction

Functional encryption [3, 16] is a generalization of public-key encryption, which allows fine-grained access control on encrypted data. In comparison to the "all-or-nothing" approach of public-key encryption schemes, functional encryption schemes allow for the generation of so-called functional decryption keys sk_f. These keys are, as the name suggests, associated with a function f and, if used in the decryption procedure, they output the associated function f applied to the underlying plaintext $f(m)$ instead of the whole plaintext m. In this setting, the function f stems from a larger functionality class F.

Due to its generality, functional encryption encompasses and unifies many of the existing advanced encryption schemes, such as identity-based encryption [2], attribute-based encryption [17], inner-product predicate encryption (IPPE) [11], and functional encryption for all polynomial-size circuits [8]. Among these, functional encryption for all polynomial-size circuits is the primitive that provides the highest functionality as it implies all of the previous ones. Unfortunately, known constructions rely on heavy mathematical tools, such as multilinear maps and indistinguishability obfuscation, making them too inefficient for practical purposes.

For the construction of more practical functional encryption schemes, it is necessary to find the right balance in the trade-off between the expressiveness of the functionality and the efficiency of the scheme. This makes it possible to rely on well established assumptions, such as DDH, k-LIN, XDLIN and LWE for example. In fact, as discussed in Deliverable D4.7, the use of lattice-based complexity assumptions (e.g. LWE) seems quite promising, since they allow for the construction of functional encryption schemes with post-quantum security.

Attribute-based encryption. The concept of attribute-based encryption (ABE) [17], introduced by Sahai and Waters, is an example of a functional encryption primitive providing a reasonable balance between expressiveness and efficiency. In particular, the encryption procedure of ABE schemes is quite flexible, allowing the encryptor to dynamically choose the set of people who will be authorized to decrypt a given ciphertext. There exist two different subclasses of attribute-based encryption, a key-policy version (KP-ABE) [9], where each ciphertext is associated with a set of attributes and each secret key is associated with an access structure and the ciphertext-policy version of ABE [18], where each secret key is associated with a set of attributes and each ciphertext is associated with an access policy. The access policies in this settings determine if a user is able to decrypt the ciphertext.

In the area of ABE schemes, the first main contribution of the FENTEC project is the proposal by Chen, Gong, Kowalczyk and Wee [5] of two new unbounded attribute-based encryption (ABE) schemes with constant-size public parameters under static assumptions in bilinear groups. Both of these constructions rely on the "bilinear entropy expansion" lemma. Besides being simpler than existing unbounded ABE schemes, the presented constructions improve significantly the state of the art in this area. The description of the "bilinear entropy expansion" lemma can be found Section 2 while the constructions are presented in Section 3.1.

Inner-product predicate encryption. Another important feature for functional encryption schemes is the full attribute-hiding property. Full attribute-hiding means that it is not possible to infer which attributes are associated with a specific key or ciphertext. Among the different primitives capable of achieving the full attribute-hiding property efficiently, inner-product predicate encryption (IPPE) seems to be the most expressive one. In these schemes, ciphertexts and secret keys are associated with vectors and the decryption procedure succeeds whenever the inner-product of these two vectors is equal to zero.

In the area of IPPE schemes, the second main contribution of the FENTEC project is the proposal by Chen, Gong and Wee [6] of two new schemes achieving adaptive security and full attribute-hiding in prime-order

bilinear groups. In particular, their schemes are more efficient than those by Okamoto and Takashima [15]. The first of these schemes is based on the standard k-LIN assumption and has shorter master public keys and shorter secret keys than those of Okamoto and Takashima's IPPE under the weaker DLIN = 2-LIN assumption. The second scheme is based on the stronger XDLIN assumption and makes it possible to shorten the ciphertext even further.

1.1 Purpose of the Document

A primary goal of this deliverable is to give an overview of the contributions made by the FENTEC partners in the area of functional encryption for expressive functionalities. Towards this goal, we present two different unbounded ABE schemes introduced by Chen, Gong, Kowalczyk and Wee [5] and two different inner-product predicate encryption schemes introduced by Chen, Gong and Wee [6] in the context of the FENTEC project. These schemes are reasonably efficient and represent the current state of the art in the area of attribute-based encryption and inner-product predicate encryption schemes.

1.2 Structure and Methodology

Section 2 recalls some of the definitions and basic tools that are used in the remainder of the document. In addition to this, we also describe the necessary complexity assumptions and cryptographic primitives, as well as the corresponding security definitions. Section 3 then describes our main contributions. These are separated into two subsections: Section 3.1, where we describe the two different unbounded ABE schemes and Section 3.2, which contains the two IPPE schemes with shorter ciphertexts. Finally, Section 4 concludes by establishing a connection between the constructed schemes and the use cases.

1.3 Relation to Deliverable 4.1

The inner-product predicate encryption scheme based on the XDLIN assumption was already described in Deliverable 4.1, since it is applicable to the video surveillance use case considered in WP7. In comparison to that deliverable, the current deliverable provides more details about the actual construction and its possible instantiations. In addition, an unbounded attribute-based encryption scheme by Chen et al. [5] is described in Section 3.1.

2 Preliminaries

In this section, we recall and extend definitions given in Deliverable 4.1, such that we can give an overview over the contributions made by the FENTEC partners.

2.1 Notation and conventions

We begin by recapping the notations, as defined in Deliverable 4.1.

Let $\mathbb{N}$ denote the set of natural numbers. 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 ε. More generally, if S is a set, then S^n is the set of n-tuples of elements of S, $S^{\leq n}$ is the set of tuples of length at most n. If x is a string then $|x|$ denotes its length, and if S is a set then $|S|$ denotes its size. If S is finite, then $x \leftarrow\!\!\$\, S$ denotes the assignment to x of an element chosen uniformly at random from S. If $\mathcal{A}$ is an algorithm, then $y \leftarrow \mathcal{A}(x)$ denotes the assignment to y of the output of $\mathcal{A}$ on input x, and if $\mathcal{A}$ is randomized, then $y \leftarrow\!\!\$\, \mathcal{A}(x)$ denotes that the output of an execution of $\mathcal{A}(x)$ with fresh coins assigned to y. Unless otherwise indicated, an algorithm may be randomized. "PPT" stands for probabilistic polynomial time and "PTA" for polynomial-time algorithm or adversary. Most of the time we denote by λ the security parameter. A function $\nu : \mathbb{N} \to [0,1]$ is said to be *negligible* if for every $c \in \mathbb{N}$ there exists a $\lambda_c \in \mathbb{N}$ such that $\nu(\lambda) \leq \lambda^{-c}$ for all $\lambda > \lambda_c$, and it is said to be *overwhelming* if the function $|1 - \nu(\lambda)|$ is negligible.

2.2 Represented groups

For the description of the different groups and group operations, we orientate on the works [6] and [5].

We use lower case boldface to denote (column) vectors and upper case boldcase to denote matrices. We use $\equiv$ to denote two distributions being identically distributed, and $\approx_c$ to denote two distributions being computationally indistinguishable. For any two finite sets (also including spaces and groups) S_1 and S_2, the notation "$S_1 \approx_c S_2$" means the uniform distributions over them are computationally indistinguishable.

Let $\mathbf{A}$ be a matrix over $\mathbb{Z}_p$. We use $\mathsf{span}(\mathbf{A})$ to denote the column span of $\mathbf{A}$, use $\mathsf{basis}(\mathbf{A})$ to denote a basis of $\mathsf{span}(\mathbf{A})$, and use $(\mathbf{A}_1|\mathbf{A}_2)$ to denote the concatenation of matrices $\mathbf{A}_1, \mathbf{A}_2$. By $\mathsf{span}(\mathbf{A}^\top)$, we are indicating the row span of $\mathbf{A}^\top$. We let $\mathbf{I}_n$ be the n-by-n identity matrix and $\mathbf{0}$ be a zero matrix of proper size. Given an invertible matrix $\mathbf{B}$, we use $\mathbf{B}^*$ to denote its dual satisfying $\mathbf{B}^\top \mathbf{B}^* = \mathbf{I}$.

A generating algorithm $GroupGen(\cdot)$ takes as input a value 1^λ related to the security parameter λ and outputs $\mathbb{G} := (G_N, H_N, G_T, e)$, where N is product of three primes p_1, p_2, p_3 of $\Theta(\lambda)$ bits, G_N, H_N and G_T are cyclic groups of order N and $e : G_N \times H_N \to G_T$ is a non-degenerate bilinear map. We require that the group operations in G_N, H_N and G_T as well the bilinear map e are computable in deterministic polynomial time with respect to λ. We assume that a random generator g (resp. h) of G_N (resp. H_N) and $t = e(g,h) \in G_T$ is always contained in the description of the bilinear groups. For every divisor n of N, we denote by G_n the subgroup of G_N of order n. We use g_1, g_2, g_3 to denote random generators of the subgroups $G_{p_1}, G_{p_2}, G_{p_3}$ respectively. We define h_1, h_2, h_3 random generators of the subgroups $H_{p_1}, H_{p_2}, H_{p_3}$ analogously. We employ the *implicit representation* of group elements: for a matrix $\mathbf{M}$ over $\mathbb{Z}_p$, we define $[\mathbf{M}]_1 := g^{\mathbf{M}}$, $[\mathbf{M}]_2 := h^{\mathbf{M}}$, $[\mathbf{M}]_T := t^{\mathbf{M}}$, where exponentiation is carried out component-wise. Also, given $[\mathbf{A}]_1, [\mathbf{B}]_2$, we let $e([\mathbf{A}]_1, [\mathbf{B}]_2) = [\mathbf{AB}]_T$.

2.3 Complexity Assumptions

This section contains a description of all the different complexity assumptions used for the ABE and IPPE constructions. The description can be separated in two parts:

1. Standard assumptions like MDDH and XDLIN. This section also contains a description of monotone span programs;
2. An overview of the bilinear entropy expansion lemma.

2.3.1 Standard assumptions

As already described in Section 1, we use the k-LIN assumption as the underlying hardness assumption for one of the IPPE schemes. Instead of using the k-LIN assumption directly, we use an implication the so called $\text{MDDH}_{k,\ell}$ assumption. We review the matrix Diffie-Hellman (MDDH) assumption on G_1 [7]. The assumptions on G_2 can be defined analogously and it is known that $k\text{-LIN} \Rightarrow \text{MDDH}_{k,\ell}$ [7].

Assumption 1 ($\text{MDDH}_{k,\ell}$ Assumption) *Let $\ell > k \geq 1$. We say that the $\text{MDDH}_{k,\ell}$ assumption holds with respect to $GroupGen(1^\lambda)$ if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}^{MDDH_{k,\ell}}_{\mathcal{A}}(\lambda) := \left|\Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{Ms}]_1) = 1] - \Pr[\mathcal{A}(\mathbb{G}, [\mathbf{M}]_1, [\mathbf{u}]_1) = 1]\right|$$

where $\mathbb{G} \leftarrow GroupGen(1^\lambda)$, $\mathbf{M} \leftarrow \mathbb{Z}_p^{\ell \times k}$, $\mathbf{s} \leftarrow \mathbb{Z}_p^k$ and $\mathbf{u} \leftarrow \mathbb{Z}_p^\ell$.

We also use the external decisional linear (XDLIN) assumption on G_2 [1]:

Definition 1 (eXternal Decisional LINear (XDLIN) assumption) *We say that the XDLIN assumption holds with respect to $GroupGen(1^\lambda)$ if for all PPT adversaries $\mathcal{A}$, the following advantage function is negligible in λ.*

$$\mathsf{Adv}^{\text{XDLIN}}_{\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(\mathbb{G}, D, T_0 = [a_3(s_1 + s_2)]_2) = 1] - \Pr[\mathcal{A}(\mathbb{G}, D, T_1 \leftarrow_\$ \mathbb{G}_2) = 1]|$$

where $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_t, p, g_1, g_2, e) \leftarrow_\$ GroupGen(1^\lambda)$ and $D = ([a_1, a_2, a_3, a_1 s_1, a_2 s_2]_1, [a_1, a_2, a_3, a_1 s_1, a_2 s_2]_2)$ and $a_1, a_2, a_3, s_1, s_2 \leftarrow_\$ \mathbb{Z}_p$.

We define (monotone) span programs [10].

Definition 2 (span programs [10]) *A* (monotone) span program *for attribute universe $[n]$ is a pair $(\mathbf{M}, \rho)$ where $\mathbf{M}$ is a $\ell \times \ell'$ matrix over $\mathbb{Z}_p$ and $\rho : [\ell] \to [n]$. Given $\mathbf{x} = (x_1, \ldots, x_n) \in \{0,1\}^n$, we say that*

$$\mathbf{x} \textit{ satisfies } (\mathbf{M}, \rho) \textit{ iff } \boldsymbol{1} \in \mathsf{span}\langle \mathbf{M}_{\mathbf{x}} \rangle,$$

Here, $\boldsymbol{1} := (1, 0, \ldots, 0)^\top \in \mathbb{Z}^{1 \times \ell'}$ is a row vector; $\mathbf{M}_{\mathbf{x}}$ denotes the collection of vectors $\{\mathbf{M}_j : x_{\rho(j)} = 1\}$ where $\mathbf{M}_j$ denotes the j'th row of $\mathbf{M}$; and span *refers to linear span of collection of (row) vectors over $\mathbb{Z}_p$.*

That is, $\mathbf{x}$ satisfies $(\mathbf{M}, \rho)$ iff there exists constants $\omega_1, \ldots, \omega_\ell \in \mathbb{Z}_p$ such that

$$\sum_{j : x_{\rho(j)} = 1} \omega_j \mathbf{M}_j = \mathbf{1} \tag{1}$$

Observe that the constants $\{\omega_j\}$ can be computed in time polynomial in the size of the matrix $\mathbf{M}$ via Gaussian elimination. Like in [13, 4], we need to impose a one-use restriction, that is, ρ is a permutation and $\ell = n$. By re-ordering the rows of $\mathbf{M}$, we may assume WLOG that ρ is the identity map, which we omit in the rest of this section.

Theorem 1 (statistical lemma [4]) *For any* $\mathbf{x}$ *that does not satisfy* $\mathbf{M}$*, the distributions*

$$(\{v_j\}_{j:x_j=1}, \{\mathbf{M}_j \binom{\alpha}{\mathbf{u}} + r_j v_j,\ r_j\}_{j\in[n]})$$

perfectly hide α*, where the randomness is taken over* $v_j \xleftarrow{R} \mathbb{Z}_p, \mathbf{u} \xleftarrow{R} \mathbb{Z}_p^{\ell'-1}$*, and for any fixed* $r_j \neq 0$*.*

2.3.2 Bilinear entropy expansion

The bilinear entropy expansion lemma was initially introduced in [12]. For further details, we refer to their work. We just describe the assumptions made in [5].

These assumptions consist of the $(p_1 \mapsto p_1p_2)$-subgroup decision assumption ($\mathrm{SD}^{G_N}_{p_1\mapsto p_2}$) and the p_1-subgroup Diffie-Hellman assumption ($\mathrm{DDH}^{H_N}_{p_1}$).

Assumption 2 ($\mathrm{SD}^{G_N}_{p_1\mapsto p_2}$) *We say that* $(p_1 \mapsto p_1p_2)$*-subgroup decision assumption, denoted by* $SD^{G_N}_{p_1\mapsto p_2}$*, holds if for all PPT adversaries* $\mathcal{A}$*, the following advantage function is negligible in* λ*.*

$$\mathsf{Adv}^{SD^{G_N}_{p_1\mapsto p_2}}_{\mathcal{A}}(\lambda) := \left|\Pr[\mathcal{A}(\mathbb{G}, D, T_0) = 1] - \Pr[\mathcal{A}(\mathbb{G}, D, T_1) = 1]\right|$$

where

$$D := (g_1, g_2, g_3, h_1, h_3, h_{12}), \quad h_{12} \xleftarrow{R} H_{p_1p_2}$$
$$T_0 \xleftarrow{R} \boxed{G_{p_1}},\ T_1 \xleftarrow{R} \boxed{G_{p_1p_2}}.$$

Assumption 3 ($\mathrm{DDH}^{H_N}_{p_1}$) *We say that* p_1*-subgroup Diffie-Hellman assumption, denoted by* $DDH^{H_N}_{p_1}$*, holds if for all PPT adversaries* $\mathcal{A}$*, the following advantage function is negligible in* λ*.*

$$\mathsf{Adv}^{DDH^{H_N}_{p_1}}_{\mathcal{A}}(\lambda) := \left|\Pr[\mathcal{A}(\mathbb{G}, D, T_0) = 1] - \Pr[\mathcal{A}(\mathbb{G}, D, T_1) = 1]\right|$$

where

$$D := (g_1, g_2, g_3, h_1, h_2, h_3),$$
$$T_0 := (h_1^x, h_1^y, \boxed{h_1^{xy}}),\ T_1 := (h_1^x, h_1^y, \boxed{h_1^{xy+z}}), \quad x, y, z \xleftarrow{R} \mathbb{Z}_N.$$

By symmetry, one may permute the indices for subgroups and/or exchange the roles of G_N and H_N, and define $\mathrm{SD}^{G_N}_{p_1\mapsto p_3}$, $\mathrm{SD}^{G_N}_{p_3\mapsto p_2}$, $\mathrm{SD}^{H_N}_{p_1\mapsto p_1p_2}$, $\mathrm{SD}^{H_N}_{p_1\mapsto p_3}$ and $\mathrm{DDH}^{H_N}_{p_2}$, $\mathrm{DDH}^{H_N}_{p_3}$ analogously.

Using these primitives, we can define the bilinear entropy expansion lemma.

Theorem 2 (Bilinear entropy expansion lemma) *Under the* $SD^{H_N}_{p_1\mapsto p_2}$, $SD^{H_N}_{p_1\mapsto p_3}$, $SD^{G_N}_{p_1\mapsto p_2}$, $DDH^{H_N}_{p_2}$, $SD^{G_N}_{p_1\mapsto p_3}$, $DDH^{H_N}_{p_3}$, $SD^{G_N}_{p_3\mapsto p_2}$ *assumptions, we have*

$$\left\{\begin{array}{l}\mathsf{aux} : g_1, g_1^w, g_1^{w_0}, g_1^{w_1}\\ \mathsf{ct} : g_1^s,\ \{g_1^{sw+s_j(w_0+j\cdot w_1)},\ g_1^{s_j}\}_{j\in[n]}\\ \mathsf{sk} : \{h_1^{r_jw},\ h_1^{r_j},\ h_1^{r_j(w_0+j\cdot w_1)}\}_{j\in[n]}\end{array}\right\}$$
$$\approx_c \left\{\begin{array}{l}\mathsf{aux} : g_1, g_1^w, g_1^{w_0}, g_1^{w_1}\\ \mathsf{ct} : g_1^s \cdot \boxed{g_2^s},\ \{g_1^{sw+s_j(w_0+j\cdot w_1)} \cdot \boxed{g_2^{sv_j+s_ju_j}},\ g_1^{s_j} \cdot \boxed{g_2^{s_j}}\}_{j\in[n]}\\ \mathsf{sk} : \{h_1^{r_jw} \cdot \boxed{h_2^{r_jv_j}},\ h_1^{r_j} \cdot \boxed{h_2^{r_j}},\ h_1^{r_j(w_0+j\cdot w_1)} \cdot \boxed{h_2^{r_ju_j}}\}_{j\in[n]}\end{array}\right\}$$

where

$$w, w_0, w_1 \xleftarrow{R} \mathbb{Z}_N,\ v_j, u_j \xleftarrow{R} \mathbb{Z}_N,\ s, s_j \xleftarrow{R} \mathbb{Z}_N,\ r_j \xleftarrow{R} \mathbb{Z}_N.$$

Concretely, the distinguishing advantage $\mathsf{Adv}^{ExpLem}_{\mathcal{A}}$ *is at most*

$$\begin{aligned}&\mathsf{Adv}^{sD_{p_1\mapsto p_2}^{H_N}}_{\mathcal{B}} + \mathsf{Adv}^{sD_{p_1\mapsto p_3}^{H_N}}_{\mathcal{B}'} + \mathsf{Adv}^{sD_{p_1\mapsto p_2}^{G_N}}_{\mathcal{B}''} + \mathsf{Adv}^{sD_{p_1\mapsto p_3}^{H_N}}_{\mathcal{B}'''}\\ &+ \mathsf{Adv}^{DDH_{p_2}^{H_N}}_{\mathcal{B}_0} + n\cdot\left(\mathsf{Adv}^{sD_{p_1\mapsto p_3}^{G_N}}_{\mathcal{B}_1} + \mathsf{Adv}^{DDH_{p_3}^{H_N}}_{\mathcal{B}_2} + \mathsf{Adv}^{sD_{p_3\mapsto p_2}^{G_N}}_{\mathcal{B}_4}\right.\\ &\left.+ \mathsf{Adv}^{DDH_{p_3}^{H_N}}_{\mathcal{B}_6} + \mathsf{Adv}^{sD_{p_1\mapsto p_3}^{G_N}}_{\mathcal{B}_7}\right) + \mathsf{Adv}^{DDH_{p_2}^{H_N}}_{\mathcal{B}_8}\end{aligned}$$

2.4 Cryptographic primitives

In this section, we recall the definitions for attribute-based encryption and inner-product predicate encryption schemes.

2.4.1 Attribute-based encryption

An attribute-based encryption (ABE) scheme for a predicate $\mathsf{P}(\cdot,\cdot)$ consists of four algorithms (Setup, Enc, KeyGen, Dec):

$\mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{Y}, \mathcal{M}) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm gets as input the security parameter λ, the attribute universe $\mathcal{X}$, the predicate universe $\mathcal{Y}$, the message space $\mathcal{M}$ and outputs the public parameter mpk, and the master key msk.

$\mathsf{Enc}(\mathsf{mpk}, x, m) \to \mathsf{ct}_x$. The encryption algorithm gets as input mpk, an attribute $x \in \mathcal{X}$ and a message $m \in \mathcal{M}$. It outputs a ciphertext ct_x. Note that x is public given ct_x.

$\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y) \to \mathsf{sk}_y$. The key generation algorithm gets as input msk and a value $y \in \mathcal{Y}$. It outputs a secret key sk_y. Note that y is public given sk_y.

$\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{ct}_x) \to m$. The decryption algorithm gets as input sk_y and ct_x such that $\mathsf{P}(x, y) = 1$. It outputs a message m.

Correctness. We require that for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$ such that $\mathsf{P}(x, y) = 1$ and all $m \in \mathcal{M}$,

$$\Pr[\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_y, \mathsf{Enc}(\mathsf{mpk}, x, m)) = m] = 1,$$

where the probability is taken over $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{Y}, \mathcal{M})$, $\mathsf{sk}_y \leftarrow \mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, y)$, and the coins of Enc.

Security. For a stateful adversary $\mathcal{A}$, we define the advantage function

$$\mathsf{Adv}^{\mathrm{ABE}}_{\mathcal{A}}(\lambda) := \left|\Pr\left[b = b' : \begin{array}{l}(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{Y}, \mathcal{M});\\ (x^*, m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk},\cdot)}(\mathsf{mpk});\\ b \xleftarrow{R} \{0,1\}; \mathsf{ct}_{x^*} \leftarrow \mathsf{Enc}(\mathsf{mpk}, x^*, m_b);\\ b' \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk},\cdot)}(\mathsf{ct}_{x^*})\end{array}\right] - \frac{1}{2}\right|$$

with the restriction that all queries y that $\mathcal{A}$ makes to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$ satisfies $\mathsf{P}(x^*, y) = 0$ (that is, sk_y does not decrypt ct_{x^*}). An ABE scheme is *adaptively secure* if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}^{\mathrm{ABE}}_{\mathcal{A}}(\lambda)$ is a negligible function in λ.

Unbounded ABE. An ABE scheme is *unbounded* [14] if the running time of Setup only depends on λ; otherwise, we say that it is bounded.

2.4.2 Inner-product predicate encryption

An inner-product predicate encryption (IPPE) scheme consists of four algorithms (Setup, KeyGen, Enc, Dec):

$\mathsf{Setup}(1^\lambda, n) \to (\mathsf{mpk}, \mathsf{msk})$. The setup algorithm gets as input the security parameter λ and the dimension n of the vector space. It outputs the master public key mpk and the master key msk.

$\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y}) \to \mathsf{sk}_\mathbf{y}$. The key generation algorithm gets as input msk and a vector $\mathbf{y}$. It outputs a secret key $\mathsf{sk}_\mathbf{y}$ for vector $\mathbf{y}$.

$\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m) \to \mathsf{ct}_\mathbf{x}$. The encryption algorithm gets as input mpk, a vector $\mathbf{x}$ and a message m. It outputs a ciphertext $\mathsf{ct}_\mathbf{x}$ for vector $\mathbf{x}$.

$\mathsf{Dec}(\mathsf{ct}_\mathbf{x}, \mathsf{sk}_\mathbf{y}) \to m$. The decryption algorithm gets as a ciphertext $\mathsf{ct}_\mathbf{x}$ for $\mathbf{x}$ and a secret key $\mathsf{sk}_\mathbf{y}$ for vector $\mathbf{y}$ satisfying $\langle \mathbf{x}, \mathbf{y} \rangle = 0$. It outputs message m.

Correctness. We require that for all vectors $\mathbf{x}, \mathbf{y}$ satisfying $\langle \mathbf{x}, \mathbf{y} \rangle = 0$ and all m, it holds that

$$\Pr[\mathsf{Dec}(\mathsf{ct}_\mathbf{x}, \mathsf{sk}_\mathbf{y}) = m] = 1,$$

where $(\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, n)$, $\mathsf{ct}_\mathbf{x} \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)$, $\mathsf{sk}_\mathbf{y} \leftarrow \mathsf{KeyGen}(\mathsf{msk}, \mathbf{y})$.

Security. For a stateful adversary $\mathcal{A}$, we define the advantage function

$$\mathsf{Adv}^{\mathrm{IPE}}_{\mathcal{A}}(\lambda) := \left| \Pr\left[b = b' : \begin{array}{l} (\mathsf{mpk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, n); \\ (\mathbf{x}_0, \mathbf{x}_1, m_0, m_1) \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, \cdot)}(\mathsf{mpk}); \\ b \xleftarrow{R} \{0,1\};\ \mathsf{ct}^* \leftarrow \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}_b, m_b); \\ b' \leftarrow \mathcal{A}^{\mathsf{KeyGen}(\mathsf{msk}, \cdot)}(\mathsf{ct}^*) \end{array} \right] - \frac{1}{2} \right|$$

with the following restrictions on all queries $\mathbf{y}$ that $\mathcal{A}$ submitted to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$:

- if $m_0 \neq m_1$, we require that $\langle \mathbf{x}_0, \mathbf{y} \rangle \neq 0 \wedge \langle \mathbf{x}_1, \mathbf{y} \rangle \neq 0$;
- if $m_0 = m_1$, we require that either $\langle \mathbf{x}_0, \mathbf{y} \rangle \neq 0 \wedge \langle \mathbf{x}_1, \mathbf{y} \rangle \neq 0$ or $\langle \mathbf{x}_0, \mathbf{y} \rangle = \langle \mathbf{x}_1, \mathbf{y} \rangle = 0$.

An IPPE scheme is *adaptively secure* and *fully attribute-hiding* if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}^{\mathrm{IPE}}_{\mathcal{A}}(\lambda)$ is a negligible function in λ.

Private-key IPPE. In a private-key IPPE, the Setup algorithm does not output mpk; and the Enc algorithm takes msk instead of mpk as input. The adaptive security and full attribute-hiding can be defined analogously except that $\mathcal{A}$ only gets ct^* and has access to $\mathsf{KeyGen}(\mathsf{msk}, \cdot)$. The advantage function is denoted by $\mathsf{Adv}^{\mathrm{IPE}^*}_{\mathcal{A}}(\lambda)$. Accordingly, we may call the standard IPPE *public-key IPPE*.

3 Our Contributions

In this section, we describe the improvements made on the current state of the art by FENTEC participants.

We start by describing the improvements in the field of adaptively secure unbounded ABE, these improvements includes a simple scheme in composite-order groups based on the k-LIN assumption and a scheme in prime-order groups based on the XDLIN assumption with shorter ciphertexts and keys than the first one [5].

FENTEC partners have also made contributions to the field of adaptively secure and full attribute-hiding inner-product predicate encryption (IPPE). The improvements in this area include an IPPE scheme in prime-order bilinear groups based on the k-LIN assumptions that have shorter ciphertext and keys than the only other exisiting scheme with the same properties presented by Okamoto and Takashima [15]. This scheme can also be adapted to a scheme that has even shorter ciphertexts based on the XDLIN assumption.

3.1 Unbounded Attribute-based Encryption

In [5], the authors present two different constructions for an unbounded key-policy attribute-based encryption scheme for monotone span programs [10]. Both of these constructions fulfill four different properties:

1. they are unbounded (the set-up algorithm is independent of the length of the attributes or the size of the policies);
2. they can be based on faster asymmetric prime-order bilinear groups;
3. they achieve adaptive security;
4. they rely on simple hardness assumptions in the standard model.

For the core of these constructions a "bilinear entropy expansion" lemma (Section 2.3.2) is used. This lemma allows the generation of any polynomial amount of entropy starting from constant-size public parameters. The entropy is then used to transform existing adaptively secure bounded ABE schemes into unbounded ones.

We start by describing the first scheme in the simpler setting of composite-order bilinear groups. In a final step, we describe the scheme in prime-order groups.

3.1.1 Unbounded KP-ABE in Composite-Order Groups

Now, we present the adaptively secure, unbounded KP-ABE for monotone span programs. This construction is based on static assumptions in composite-order groups.

- $\underline{\mathsf{Setup}(1^\lambda, 1^n)}$: On input $(1^\lambda, 1^n)$, sample $\mathbb{G} := (N = p_1p_2p_3, G_N, H_N, G_T, e) \leftarrow \mathcal{G}(1^\lambda)$ and select random generators g_1, h_1 and h_{123} of G_{p_1}, H_{p_1} and H_N, respectively. Pick

$$w, w_0, w_1 \xleftarrow{R} \mathbb{Z}_N,\ \alpha \xleftarrow{R} \mathbb{Z}_N,$$

  a pairwise independent hash function $\mathsf{H} : G_T \to \{0,1\}^\lambda$, and output the master public and secret key pair

$$\mathsf{mpk} := \left((N, G_N, H_N, G_T, e);\ g_1,\ g_1^w,\ g_1^{w_0},\ g_1^{w_1},\ e(g_1, h_{123})^\alpha;\ \mathsf{H} \right)$$
$$\mathsf{msk} := (h_{123}, h_1, \alpha, w, w_0, w_1\ ).$$

- Enc(mpk, $\mathbf{x}, m$): On input an attribute vector $\mathbf{x} := (x_1, \ldots, x_n) \in \{0,1\}^n$ and $m \in \{0,1\}^\lambda$, pick $s, s_j \xleftarrow{R} \mathbb{Z}_N$ for all $j \in [n]$ and output

$$\mathsf{ct}_{\mathbf{x}} := \Big(C_0 := g_1^s,\ \{\ C_{1,j} := g_1^{sw+s_j(w_0+j\cdot w_1)},\ C_{2,j} := g_1^{s_j}\ \}_{j:x_j=1}, C := \mathsf{H}(e(g_1,h_{123})^{\alpha s}) \cdot m \Big).$$

- KeyGen(mpk, msk, $\mathbf{M}$): On input a monotone span program $\mathbf{M} \in \mathbb{Z}_N^{n\times \ell'}$, pick $\mathbf{u} \xleftarrow{R} \mathbb{Z}_N^{\ell'-1}$ and $r_j \xleftarrow{R} \mathbb{Z}_N$ for all $j \in [n]$, and output

$$\mathsf{sk}_{\mathbf{M}} := \big(\{\ K_{0,j} := h_{123}^{\mathbf{M}_j\binom{\alpha}{\mathbf{u}}} \cdot h_1^{r_j w},\ K_{1,j} := h_1^{r_j},\ K_{2,j} := h_1^{r_j(w_0+j\cdot w_1)}\ \}_{j\in[n]} \big) \in H_N^{3n}.$$

- Dec(mpk, $\mathsf{sk}_{\mathbf{M}}$, $\mathsf{ct}_{\mathbf{x}}$): If $\mathbf{x}$ satisfies $\mathbf{M}$, compute $\omega_1, \ldots, \omega_n \in \mathbb{Z}_p$ such that

$$\textstyle\sum_{j:x_j=1} \omega_j \mathbf{M}_j = \mathbf{1}.$$

  Then, compute

$$K \leftarrow \textstyle\prod_{j:x_j=1} \big(e(C_0, K_{0,j}) \cdot e(C_{1,j}, K_{1,j})^{-1} \cdot e(C_{2,j}, K_{2,j})\big)^{\omega_j},$$

  and recover the message as $m \leftarrow C/\mathsf{H}(K) \in \{0,1\}^\lambda$.

The correctness can be easily proven, hence we omit the details here and refer to [5].

Security. Adaptive security of the scheme described above means that the adversary is allowed to choose the input on which it wishes to be challenged at any time in the security experiment. As shown in [5], the following security bound holds for this scheme:

Theorem 3 *For any adversary $\mathcal{A}$ that makes at most Q key queries against the unbounded KP-ABE scheme, there exist adversaries $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that:*

$$\mathsf{Adv}^{ABE}_{\mathcal{A}}(\lambda) \le \mathsf{Adv}^{ExpLem}_{\mathcal{B}_0} + \mathsf{Adv}^{sD^{G_N}_{p_2\mapsto p_3}}_{\mathcal{B}_1} + Q \cdot \mathsf{Adv}^{sD^{H_N}_{p_2\mapsto p_3}}_{\mathcal{B}_2} + Q \cdot \mathsf{Adv}^{sD^{H_N}_{p_2\mapsto p_3}}_{\mathcal{B}_3}$$

where In particular, we achieve security loss $O(n+Q)$ based on the $sD^{H_N}_{p_1\mapsto p_2}$, $sD^{H_N}_{p_1\mapsto p_3}$, $sD^{G_N}_{p_1\mapsto p_2}$, $DDH^{H_N}_{p_2}$, $sD^{G_N}_{p_1\mapsto p_3}$, $DDH^{H_N}_{p_3}$, $sD^{G_N}_{p_3\mapsto p_2}$, $sD^{G_N}_{p_2\mapsto p_3}$, $sD^{H_N}_{p_2\mapsto p_3}$ assumptions.

The full details of the proof of Theorem 3 can be found in [5].

3.1.2 Unbounded KP-ABE in Prime-Order Groups

In this section, we present another adaptively secure unbounded KP-ABE for monotone span programs programs. Instead of relying on it is based on the MDDH assumption in prime-order groups.

- Setup($1^\lambda, 1^n$): On input $(1^\lambda, 1^n)$, sample $\mathbf{A}_1 \xleftarrow{R} \mathbb{Z}_p^{(2k+1)\times k}, \mathbf{B} \xleftarrow{R} \mathbb{Z}_p^{(k+1)\times k}$ and

$$\mathbf{W}, \mathbf{W}_0, \mathbf{W}_1 \xleftarrow{R} \mathbb{Z}_p^{(2k+1)\times(k+1)},\ \mathbf{k} \xleftarrow{R} \mathbb{Z}_p^{2k+1}$$

  and output the master public and secret key pair

$$\mathsf{mpk} := \big(\ [\mathbf{A}_1^\top, \mathbf{A}_1^\top\mathbf{W}, \mathbf{A}_1^\top\mathbf{W}_0, \mathbf{A}_1^\top\mathbf{W}_1]_1,\ e([\mathbf{A}_1^\top]_1, [\mathbf{k}]_2)\ \big)$$
$$\mathsf{msk} := (\ \mathbf{k},\ \mathbf{B},\ \mathbf{W},\ \mathbf{W}_0,\ \mathbf{W}_1\ ).$$

- $\underline{\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}, m)}$: On input an attribute vector $\mathbf{x} := (x_1, \ldots, x_n) \in \{0,1\}^n$ and $m \in G_T$, pick $\mathbf{c}, \mathbf{c}_j \xleftarrow{R} \mathsf{span}(\mathbf{A}_1)$ for all $j \in [n]$ and output

$$\mathsf{ct}_{\mathbf{x}} := \left(\begin{array}{l} C_0 := [\mathbf{c}^\top]_1, \\ \{\ C_{1,j} := [\mathbf{c}^\top \mathbf{W} + \mathbf{c}_j^\top (\mathbf{W}_0 + j \cdot \mathbf{W}_1)]_1, C_{2,j} := [\mathbf{c}_j^\top]_1\ \}_{j:x_j=1}, \\ C := e([\mathbf{c}^\top]_1, [\mathbf{k}]_2) \cdot m \end{array} \right) \in G_1^{2k+1} \times (G_1^{k+1} \times G_1^{2k+1})^n \times G_T.$$

- $\underline{\mathsf{KeyGen}(\mathsf{mpk}, \mathsf{msk}, \mathbf{M})}$: On input a monotone span program $\mathbf{M} \in \mathbb{Z}_p^{n \times \ell'}$, pick $\mathbf{K}' \xleftarrow{R} \mathbb{Z}_p^{(2k+1)\times(\ell'-1)}$, $\mathbf{d}_j \xleftarrow{R} \mathsf{span}(\mathbf{B})$ for all $j \in [n]$, and output

$$\mathsf{sk}_{\mathbf{M}} := \left(\left\{ \begin{array}{c} K_{0,j} := [(\mathbf{k} \| \mathbf{K}')\mathbf{M}_j^\top + \mathbf{W}\mathbf{d}_j]_2,\ K_{1,j} := [\mathbf{d}_j]_2, \\ K_{2,j} := [(\mathbf{W}_0 + j \cdot \mathbf{W}_1)\mathbf{d}_j]_2 \end{array} \right\}_{j \in [n]} \right) \in (G_2^{2k+1} \times G_2^{k+1} \times G_2^{2k+1})^n.$$

- $\underline{\mathsf{Dec}(\mathsf{mpk}, \mathsf{sk}_{\mathbf{M}}, \mathsf{ct}_{\mathbf{x}})}$: If $\mathbf{x}$ satisfies $\mathbf{M}$, compute $\omega_1, \ldots, \omega_n \in \mathbb{Z}_p$ such that

$$\textstyle\sum_{j:x_j=1} \omega_j \mathbf{M}_j = \mathbf{1}.$$

  Then, compute

$$K \leftarrow \textstyle\prod_{j:x_j=1} \left(e(C_0, K_{0,j}) \cdot e(C_{1,j}, K_{1,j})^{-1} \cdot e(C_{2,j}, K_{2,j}) \right)^{\omega_j},$$

  and recover the message as $m \leftarrow C/K \in G_T$.

The proof of correctness is straightforward, we omit it here and refer to [5].

Security

The bound for the adaptive security under key generation queries is the following:

Theorem 4 *For any adversary $\mathcal{A}$ that makes at most Q key queries against the unbounded KP-ABE scheme, there exist adversaries $\mathcal{B}_0, \mathcal{B}_1, \mathcal{B}_2$ such that:*

$$\mathsf{Adv}^{ABE}_{\mathcal{A}}(\lambda) \leq \mathsf{Adv}^{ExpLemRev}_{\mathcal{B}_0} + Q \cdot \mathsf{Adv}^{MDDH^n_{k,k+1}}_{\mathcal{B}_1} + Q \cdot \mathsf{Adv}^{MDDH^n_{k,k+1}}_{\mathcal{B}_2} + O(1/p).$$

In particular, we achieve security loss $O(n+Q)$ based on the $\textsc{mddh}_k$ assumption.

A detailed proof of the Theorem is presented in [5].

3.2 Improved Inner-product Predicate Encryption

In [6], the authors present two different IPPE schemes that achieve adaptive security and full attribute-hiding the prime-order bilinear group.

1. A scheme based on the standard k-LIN assumption that has shorter master public and secret keys than previous constructions in the same setting;
2. An adaption of the first scheme that is based on the XDLIN assumption instead of the k-LIN assumption and through this provides shorter ciphertexts compared to the first one.

Both of these schemes are constructed in the private and the public key setting. In this deliverable only the private key schemes are presented. The public keys schemes can be directly derived from the private key schemes by applying the transformation described in [19]. For further details we refer to [6].

We start by describing the first scheme based on the k-LIN assumption. The second step consists of the adaption under the XDLIN assumption.

3.2.1 Inner-product Predicate Encryption Scheme based on the k-LIN assumption

Now, we present the first construction in prime-order bilinear groups, based on the k-LIN assumption:

- $\underline{\mathsf{Setup}(1^\lambda, n)}$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow GroupGen(1^\lambda)$. Sample $\mathbf{B}_1 \leftarrow \mathbb{Z}_p^{(2k+1)\times k}$ and pick $\mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n \leftarrow \mathbb{Z}_p^{1\times(2k+1)}$, $\alpha \leftarrow \mathbb{Z}_p$. Output

$$\mathsf{msk} = (\mathbb{G}, \alpha, \mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n, \mathbf{B}_1).$$

- $\underline{\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y})}$: Let $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$. Sample $\mathbf{r} \leftarrow \mathbb{Z}_p^k$ and output

$$\mathsf{sk}_\mathbf{y} = (K_0 = [\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{B}_1\mathbf{r}]_2,\ K_1 = [\mathbf{B}_1\mathbf{r}]_2)$$

- $\underline{\mathsf{Enc}(\mathsf{msk}, \mathbf{x}, m)}$: Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ and $m \in G_2$. Output

$$\mathsf{ct}_\mathbf{x} = (C_1 = x_1 \cdot \mathbf{u} + \mathbf{w}_1,\ \ldots,\ C_n = x_n \cdot \mathbf{u} + \mathbf{w}_n,\ C = [\alpha]_2 \cdot m)$$

- $\underline{\mathsf{Dec}(\mathsf{ct}_\mathbf{x}, \mathsf{sk}_\mathbf{y})}$: Parse $\mathsf{ct}_\mathbf{x} = (C_1, \ldots, C_n, C)$ and $\mathsf{sk}_\mathbf{y} = (K_0, K_1)$ for $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$. Output

$$m' = C \cdot ((y_1 \cdot C_1 + \cdots + y_n \cdot C_n) \odot K_1) \cdot K_0^{-1}.$$

The proof of correctness is straightforward, hence we omit it here and refer to [6].

Security. The scheme described above is adaptively secure and full attribute hiding under the k-LIN assumption. In the security proof of this scheme, the following bounds are determined:

Theorem 5 *For any adversary $\mathcal{A}$ that makes at most Q queries and outputs $m_0 = m_1$, there exists PPT adversaries $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that*

$$\mathsf{Adv}^{IPE^*}_{\mathcal{A}}(\lambda) \le Q \cdot \mathsf{Adv}^{SD^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_3}}_{\mathcal{B}_1}(\lambda) + Q \cdot \mathsf{Adv}^{SD^{G_2}_{\mathbf{B}_3 \mapsto \mathbf{B}_3, \mathbf{B}_2}}_{\mathcal{B}_2}(\lambda) + Q \cdot \mathsf{Adv}^{SD^{G_2}_{\mathbf{B}_1 \mapsto \mathbf{B}_1, \mathbf{B}_3}}_{\mathcal{B}_3}(\lambda).$$

A detailed proof of the Theorem is provided in [6].

3.2.2 Inner-product Predicate Encryption Scheme based on the XDLIN assumption

The scheme above can be adapted into another scheme that has a shorter ciphertext size. To achieve this, we need to rely on the XDLIN assumptions instead of the k-LIN assumption. The resulting scheme has the following structure.

- Setup$(1^\lambda, n)$: Run $\mathbb{G} = (p, G_1, G_2, G_T, e) \leftarrow GroupGen(1^\lambda)$. Sample $\mathbf{B}_{14} = (\mathbf{B}_1|\mathbf{B}_4) \leftarrow \mathbb{Z}_p^{4\times 2}$ and pick $\mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n \leftarrow \mathbb{Z}_p^{1\times 4}$, $\alpha \leftarrow \mathbb{Z}_p$. Output

$$\mathsf{msk} = (\mathbb{G}, \alpha, \mathbf{u}, \mathbf{w}_1, \ldots, \mathbf{w}_n, \mathbf{B}_{14}).$$

- KeyGen(msk, $\mathbf{y}$): Let $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$. Sample $\mathbf{r} \leftarrow \mathbb{Z}_p^2$ and output

$$\mathsf{sk}_\mathbf{y} = (K_0 = [\alpha + (y_1 \cdot \mathbf{w}_1 + \cdots + y_n \cdot \mathbf{w}_n)\mathbf{B}_{14}\mathbf{r}]_2,\ K_1 = [\mathbf{B}_{14}\mathbf{r}]_2)$$

- Enc(msk, $\mathbf{x}, m$): Let $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ and $m \in G_T$. Output

$$\mathsf{ct}_\mathbf{x} = (C_1 = [x_1 \cdot \mathbf{u} + \mathbf{w}_1]_1,\ \ldots,\ C_n = [x_n \cdot \mathbf{u} + \mathbf{w}_n]_1,\ C = [\alpha]_T \cdot m)$$

- Dec($\mathsf{ct}_\mathbf{x}, \mathsf{sk}_\mathbf{y}$): Parse $\mathsf{ct}_\mathbf{x} = (C_1, \ldots, C_n, C)$ and $\mathsf{sk}_\mathbf{y} = (K_0, K_1)$ for $\mathbf{y} = (y_1, \ldots, y_n) \in \mathbb{Z}_p^n$. Output

$$m' = C \cdot e(y_1 \odot C_1 \cdots y_n \odot C_n, K_1) \cdot e([1]_1, K_0)^{-1}.$$

Correctness can be easily shown, hence we omit it here and refer to [6].

Security. The scheme described above is proven secure in the same setting as the other IPPE scheme. The adaptive security holds within the following bound:

Theorem 6 *For any adversary $\mathcal{A}$ that makes at most Q key queries and outputs $m_0 = m_1$, there exists adversaries $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$ such that*

$$\mathsf{Adv}^{IPE^*}_{\mathcal{A}}(\lambda) \leq Q \cdot \mathsf{Adv}^{SD^{G_2}_{\mathbf{B}_1,\mathbf{B}_4\mapsto\mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}}_{\mathcal{B}_1}(\lambda) + Q \cdot \mathsf{Adv}^{XSD^{G_2}_{\mathbf{B}_3,\mathbf{B}_4\mapsto\mathbf{B}_2,\mathbf{B}_3,\mathbf{B}_4}}_{\mathcal{B}_2}(\lambda)$$
$$+ Q \cdot \mathsf{Adv}^{SD^{G_2}_{\mathbf{B}_1,\mathbf{B}_4\mapsto\mathbf{B}_1,\mathbf{B}_3,\mathbf{B}_4}}_{\mathcal{B}_3}(\lambda).$$

A detailed proof of Theorem 6 can be found in [6].

4 Conclusion

In this document, we described two unbounded attribute-based encryption schemes and two inner-product predicate encryption schemes developed in the context of the FENTEC project. In particular, the two unbounded attribute-based encryption schemes in Section 3.1 are based on the bilinear entropy expansion lemma and represent the current state of the art in this area. Likewise, the two inner-product predicate encryption schemes presented in Section 3.2 are based on the DLIN and the XDLIN assumption and are currently the most efficient such schemes.

As already mentioned in Deliverable 4.1, the proposed inner-product predicate encryption schemes in Section 3.2 fit the video surveillance use case, considered in WP7, very well. Due to the short ciphertexts achieved by these constructions, it is possible to handle the data produced by the different video cameras in the required time.

References

[1] Masayuki Abe, Melissa Chase, Bernardo David, Markulf Kohlweiss, Ryo Nishimaki, and Miyako Ohkubo. Constant-size structure-preserving signatures: Generic constructions and simple assumptions. In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology – ASIACRYPT 2012*, volume 7658 of *Lecture Notes in Computer Science*, pages 4–24, Beijing, China, December 2–6, 2012. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-34961-4_3. (Page 4.)

[2] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003. (Page 1.)

[3] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *TCC 2011: 8th Theory of Cryptography Conference*, volume 6597 of *Lecture Notes in Computer Science*, pages 253–273, Providence, RI, USA, March 28–30, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-19571-6_16. (Pages iv and 1.)

[4] Jie Chen, Romain Gay, and Hoeteck Wee. Improved dual system ABE in prime-order groups via predicate encodings. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology – EUROCRYPT 2015, Part II*, volume 9057 of *Lecture Notes in Computer Science*, pages 595–624, Sofia, Bulgaria, April 26–30, 2015. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-46803-6_20. (Pages 4 and 5.)

[5] Jie Chen, Junqing Gong, Lucas Kowalczyk, and Hoeteck Wee. Unbounded ABE via bilinear entropy expansion, revisited. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 503–534, Tel Aviv, Israel, April 29 – May 3, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-78381-9_19. (Pages iv, 1, 2, 3, 5, 8, 9, and 10.)

[6] Jie Chen, Junqing Gong, and Hoeteck Wee. Improved inner-product encryption with adaptive security and full attribute-hiding. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018, Part II*, volume 11273 of *Lecture Notes in Computer Science*, pages 673–702, Brisbane, Queensland, Australia, December 2–6, 2018. Springer, Heidelberg, Germany. doi:10.1007/978-3-030-03329-3_23. (Pages iv, 1, 2, 3, 11, and 12.)

[7] Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013, Part II*, volume 8043 of *Lecture Notes in Computer Science*, pages 129–147, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-40084-1_8. (Page 4.)

[8] Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th Annual Symposium on Foundations of Computer Science*, pages 40–49, Berkeley, CA, USA, October 26–29, 2013. IEEE Computer Society Press. doi:10.1109/FOCS.2013.13. (Pages iv and 1.)

[9] Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. Attribute-based encryption for fine-grained access control of encrypted data. In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 06: 13th Conference on Computer and Communications Security*,

pages 89–98, Alexandria, Virginia, USA, October 30 – November 3, 2006. ACM Press. Available as Cryptology ePrint Archive Report 2006/309. doi:10.1145/1180405.1180418. (Page 1.)

[10] Mauricio Karchmer and Avi Wigderson. On span programs. In *Proceedings of the Eigth Annual Structure in Complexity Theory Conference, San Diego, CA, USA, May 18-21, 1993*, pages 102–111. IEEE Computer Society, 1993. URL: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=920, doi:10.1109/SCT.1993.336536. (Pages 4 and 8.)

[11] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. *Journal of Cryptology*, 26(2):191–224, April 2013. doi:10.1007/s00145-012-9119-4. (Pages iv and 1.)

[12] Lucas Kowalczyk and Allison Bishop Lewko. Bilinear entropy expansion from the decisional linear assumption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *Advances in Cryptology – CRYPTO 2015, Part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 524–541, Santa Barbara, CA, USA, August 16–20, 2015. Springer, Heidelberg, Germany. doi:10.1007/978-3-662-48000-7_26. (Page 5.)

[13] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 62–91, French Riviera, May 30 – June 3, 2010. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-13190-5_4. (Page 4.)

[14] Allison B. Lewko and Brent Waters. Unbounded HIBE and attribute-based encryption. In Kenneth G. Paterson, editor, *Advances in Cryptology – EUROCRYPT 2011*, volume 6632 of *Lecture Notes in Computer Science*, pages 547–567, Tallinn, Estonia, May 15–19, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-20465-4_30. (Page 7.)

[15] Tatsuaki Okamoto and Katsuyuki Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology – EUROCRYPT 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 591–608, Cambridge, UK, April 15–19, 2012. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-29011-4_35. (Pages iv, 2, and 8.)

[16] Adam O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010. http://eprint.iacr.org/2010/556. (Pages iv and 1.)

[17] Amit Sahai and Brent R. Waters. Fuzzy identity-based encryption. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473, Aarhus, Denmark, May 22–26, 2005. Springer, Heidelberg, Germany. doi:10.1007/11426639_27. (Pages iv and 1.)

[18] Brent Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors, *PKC 2011: 14th International Conference on Theory and Practice of Public Key Cryptography*, volume 6571 of *Lecture Notes in Computer Science*, pages 53–70, Taormina, Italy, March 6–9, 2011. Springer, Heidelberg, Germany. doi:10.1007/978-3-642-19379-8_4. (Page 1.)

[19] Hoeteck Wee. Attribute-hiding predicate encryption in bilinear groups, revisited. In Yael Kalai and Leonid Reyzin, editors, *TCC 2017: 15th Theory of Cryptography Conference, Part I*, volume 10677

of *Lecture Notes in Computer Science*, pages 206–233, Baltimore, MD, USA, November 12–15, 2017. Springer, Heidelberg, Germany. doi:10.1007/978-3-319-70500-2_8. (Page 11.)