A SURVEY ON FUNCTIONAL ENCRYPTION

Carla Mascia, Massimiliano Sala and Irene Villa*

University of Trento
Via Sommarive 14, Povo, Trento, Italy

(Communicated by Sihem Mesnager)

Abstract. Functional Encryption (FE) expands traditional public-key encryption in two different ways: it supports fine-grained access control and allows learning a function of the encrypted data. In this paper, we review all FE classes, describing their functionalities and main characteristics. In particular, we mention several schemes for each class, providing their security assumptions and comparing their properties. To our knowledge, this is the first survey that encompasses the entire FE family.

1. Introduction

Recent emerging applications, such as cloud services, highlight the need for a more complex notion of encryption than public-key encryption. Standard public-key encryption has an "all-or-nothing" access to encrypted data; that is, either a user can decrypt and read a secret message (plaintext), or the user will not get any further information about it in addition to what they already know from the encrypted message (ciphertext). Nevertheless, in some situations, we may want the receiver to know only some partial information of the plaintext. Or we may restrict the decryption of ciphertext to individuals who satisfy specific requirements, whereas traditional public-key encryption provides only coarse-grained access to encrypted data, where a single private key can decrypt all data.

In 1984, Shamir [163] proposes the concept of *Identity-Based cryptography* as a way to simplify certificate management in email systems. Users' identifier information, such as email addresses, can be used as public keys for encryption, so it is possible to encrypt a message to any user whose email address is known. The receiver requests a decryption key (related to its identity) to an authority or a third party and then decrypts the received ciphertext. The first practical realisations are presented in 2001, by Boneh and Franklin [40], and by Cocks [71]. In 2005, Sahai and Waters [160] introduce the *Fuzzy Identity-Based Encryption*, a generalisation of the system proposed by Shamir. The following year, Goyal, Pandey, Sahai, and Waters [103] propose the more general class of *Attribute-Based Encryption*, where

---

the access to encrypted data is given only to users with specific attributes or policies. This is the first realisation of fine-grained access control over a cryptographic system.

Later in 2007, Boneh and Waters [50] propose the so-called class of *Hidden Vector Encryption*, allowing comparison and subset queries. Katz, Sahai, and Waters [110] in 2008 present an *Inner-Product Predicate Encryption* scheme, allowing more complex queries such as evaluation of polynomials. Finally, in 2010 O'Neill [146] and in 2011 Boneh, Sahai and Waters [47] introduce the concept of *Functional Encryption*, shortly FE. This new broad vision of encryption systems comprehends all the systems as mentioned above. FE expands the functionalities of traditional public-key encryption in two different ways. First, as we have seen, it supports access control policies, allowing only users who satisfy a certain procedure to decrypt the secret information. Secondly, it permits selective computations on the ciphertexts, allowing users to learn a function of the encrypted data. In 2015, Abdalla, Bourse, De Caro, and Pointcheval [2] present the first scheme of FE that outputs a functionality of the encrypted message: *Inner Product Encryption*.

In an FE scheme, there are different keys with different roles. In general, a *public key* is generated to allow anyone in the system to encrypt any private message m. *Functional decryption keys*, also referred to as *secret keys*, are generated from a *master key*, which is supposed to be secret and kept by an authority. Each decryption key is associated with a specific function f. Decrypting an encryption of a message m with a secret key associated to a function f reveals directly the value $f(m)$. There also exists a different scenario, called *private-key setting*, where the key used to encrypt a message is not publicly known. The security of an FE scheme is based on the following: even though an adversary has access to functional decryption keys for different functionalities, it will not learn anything more than what each individual functional decryption key allows to know.

Due to its expressive access control, FE has many applications in practical situations, such as large organisations, where data is often shared according to some access policy. FE also comprehends *Searchable Encryption*, one of the active research trends in cryptography. Searchable encryption, also known as *Public-key Encryption with Keyword Search* [39], allows searching a piece of information over encrypted data while keeping the data content and the query secret even from the server holding the encrypted data. When storing sensitive data on remote servers, this guarantees the secrecy of users' sensitive data while preserving searchability on the server-side. FE can also be used for mining large datasets. It is beneficial when data is highly sensitive, for example, medical data, but revealing some partial or aggregated information on this data does not compromise the privacy of the "data-owner". This can be exploited, for example, to perform statistical analysis for medical research.

As mentioned, one of the fundamental ideas behind FE is to learn a function of the original message. Another cryptographic notion which achieves a similar result is *Fully Homomorphic Encryption* (FHE) [93]. Intriguingly, FE and FHE seem somehow intertwined, as recognised in [88, 18]. A notable difference between FE and FHE is the way the functions are applied. FE grants control over which functions can be applied to the data via a master-key holder, who issues secret keys based on the appropriateness of the function. The user then uses the secret key to obtain a function of the plaintext in the clear. Whereas FHE permits functions to

be run by anyone with the so-called *evaluation key*, but the result is still encryption. Therefore, only the owner of the secret key can decrypt the result.

Yet, the concepts of FHE and FE do have some overlap, and it has been demonstrated that functional encryption might work as FHE, with some slight adaptation [18].

OUR CONTRIBUTION. In this paper, we survey the families of functional encryption schemes. Our work aims to give the reader a wide overview of FE schemes and provide a satisfying summary of state-of-art. In particular, we focus on the functionalities of different FE schemes describing their limitations, their security models, and the mathematical assumptions involved. We also present proof of some implications among these assumptions. Given the vast literature, we do not provide detailed descriptions of the existing constructions of FE schemes; instead, we illustrate here the main ideas upon which these schemes are based, and we provide some of the most relevant and recent works. In addition, we present an overview of "non-standard" FE schemes, that is, FE schemes that go beyond the inner product encryption and schemes with enhanced properties. Indeed, in real scenarios, some characteristics of "standard" FE are not desirable, such as having unique authority. Hence schemes with more complex features have been studied and proposed, such as decentralised or multi-authority schemes.

ORGANIZATION. The survey is organized as follows. Sections 2 and 3 are both devoted to introducing preliminaries. In particular, first, we give the definition of Functional Encryption and Predicate Encryption, the latter being a large class of FE. Then, we provide a systematic presentation of the main mathematical assumptions used to prove the security of FE schemes, underlining the relations between some of them. Section 4 briefly presents the two most used models of security for an FE scheme: indistinguishability-based security and simulation-based security. Section 5 gives an overview of the well-known classes of Identity-Based Encryption and Attribute-Based Encryption. Section 6 focuses on the class of Predicate Encryption and Section 7 describes the class of Inner Product Encryption. In Section 8, we present many different generalisations of the previous schemes. Finally, in Section 9 we draw our conclusions.

2. NOTATIONS AND DEFINITION OF FE

In this section, we collect all the notations and preliminaries needed for the rest of this work.

When we talk about algorithms or adversaries, we refer to Turing machines. The acronym PPT stands for *Probabilistic Polynomial Time*, so a PPT algorithm is a probabilistic Turing machine, equipped with an extra randomness tape, that solves problems in polynomial time.

Let $n \in \mathbb{N}$, $\mathbb{Z}_n$ stands for the ring of integers modulo n and $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$.

Definition 2.1. A function $f : \mathbb{N} \to \mathbb{R}$ is called *negligible* if for any positive integer d there exists an integer N_d such that $|f(k)| < \frac{1}{k^d}$ for any $k \geq N_d$.

To define a functional encryption scheme, we follow the definition given in [47], which is the first attempt to formalise FE.

Definition 2.2. Let K be the key space containing a special key ϵ, called the *empty key*, and X be the plaintext space. A *functionality* F defined over $K \times X$ is a function $F : K \times X \to Y$, where Y is the output space containing a "fail"

character $\perp$. A *functional encryption scheme* for the functionality F is a tuple of four PPT algorithms (`Setup`, `KeyGen`, `Enc`, `Dec`) satisfying the following conditions for all $k \in K$ and all $x \in X$:

$\texttt{Setup}(1^\lambda) \to (\mathrm{pp}, \mathrm{mk})$ on input the security parameter λ, outputs a public key pp and a private key mk, called *master key*;

$\texttt{KeyGen}(\mathrm{mk}, k) \to \mathrm{sk}_k$ on input the master key mk and a key $k \in K$, outputs a secret key sk_k;

$\texttt{Enc}(\mathrm{pp}, x) \to c$ on input the public key pp and a message $x \in X$, outputs a ciphertext c;

$\texttt{Dec}(\mathrm{sk}_k, c) \to y$ on input a secret key sk_k and a ciphertext c, outputs y

where we require that $y = F(k, x)$ with probability 1.

The special key ϵ captures all the information about the plaintext that intentionally leaks from the ciphertext. Thus, if a user runs $\texttt{Dec}(\epsilon, c)$ on a ciphertext $c = \texttt{Enc}(\mathrm{pp}, x)$, it will obtain all the information about x that intentionally are revealed from c. For example, if `Enc` outputs a ciphertext of the same length as the plaintext, then the encrypted message intentionally reveals $\texttt{len}(x)$, namely the size of the plaintext.

Remark 1. Standard public-key encryption is the simplest example of functional encryption. With $K = \{1, \epsilon\}$, for $k = 1$ we get the decryption of a valid ciphertext, that is,

$$F(k, x) = \begin{cases} x & \text{if } k = 1, \\ \texttt{len}(x) & \text{if } k = \epsilon. \end{cases}$$

Remark 2. Given a functionality F, let $\mathcal{F} = \{f_k \mid k \in K \text{ and } f_k(\cdot) = F(k, \cdot)\}$ be a family of functions derived from F. An FE scheme can be defined starting from $\mathcal{F}$, instead of F, and the resulting scheme is the same as that presented in Definition 2.2. In an FE scheme for $\mathcal{F}$, the `Setup` and `Enc` algorithms are defined as in Definition 2.2, whereas `KeyGen` takes in input the master key and a function $f \in \mathcal{F}$, it outputs a secret key sk_f. The decryption algorithm, using sk_f on the encryption of x returns $f(x)$, that is, a function of the plaintext x.

Remark 3. For some practical applications, it is relevant to distinguish between *public-key* and *private-key setting*. In the former, anyone can encrypt using the public key generated in the `Setup` phase; in the latter, only those who own the master key can encrypt. Notice that the definition of FE scheme in Definition 2.2 is given in the public-key setting.

Regarding the notion of security for an FE scheme, we dedicate a separate section, see Section 4.

Many of the FE schemes present in the literature belong to the class of *predicate encryption*, a powerful tool that enables fine-grained access to encrypted information such as searching on encrypted data. Regarding the notion of security for an FE scheme, we dedicate a separate section, see Section 4.

Definition 2.3. A *predicate* is a Boolean-valued function $f : A \to \{0, 1\}$, where A is an arbitrary set, and the elements 0 and 1 of the codomain are interpreted as the logical values *false* and *true*, respectively.

In many applications, a plaintext $x \in X$ is a pair $(\mathrm{ind}, m) \in I \times M$, where I is called *index set* and M is called *payload set*. A *Predicate Encryption* (PE) scheme

is then defined in terms of a polynomial-time predicate $P : K \times I \to \{0, 1\}$ and the functionality over $K \times (I \times M)$ is defined as

$$F(k \in K \setminus \{\epsilon\}, (\text{ind}, m)) = \begin{cases} m & \text{if } P(k, \text{ind}) = 1, \\ \bot & \text{if } P(k, \text{ind}) = 0. \end{cases}$$

FE schemes can be divided into three large classes, depending on the features and functionalities they achieve:

- Predicate encryption systems with public index;
- Predicate encryption systems with private index;
- Functional encryption systems beyond predicates.

In the public-index class, the plaintext index is easily readable from the ciphertext, formally by evaluating F in the empty key ϵ. And among these schemes, one finds Identity-Based Encryption (IBE) and Attribute-Based Encryption (see Section 5). We refer to the schemes with private index simply with Predicate Encryption (PE), and among them, one finds Anonymous IBE, Hidden Vector Encryption (HVE), and Inner Product Predicate Encryption (see Section 6). Finally, the last class includes Inner Product Encryption (see Section 7).

3. MATHEMATICAL BACKGROUND AND ASSUMPTIONS

This section presents some of the main assumptions used to prove the security of FE schemes mentioned in this work.

In general, a security assumption is based on the hardness of solving a specific problem. With *hardness* we mean that an adversary (which is a PPT algorithm) can solve the problem only with a negligible probability. We will also use *intractable*, *difficult*, or *challenging* as synonyms for hard.

In this paper, q denotes a prime number, with $q \geq 5$.

3.1. BILINEAR GROUPS. In this subsection, we describe some problems and assumptions related to bilinear groups studied and used in FE schemes. Some of the problems presented in the following are formulated in the symmetric case, the others in the more general asymmetric setting.

Definition 3.1. A *bilinear group* is a tuple $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ such that:

- $\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T$ are (multiplicative) cyclic groups of prime order q where the group actions can be computed efficiently;
- $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is a *bilinear* map, that is, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$, for all g_1, g_2 elements in $\mathbb{G}_1, \mathbb{G}_2$, respectively, and all a, b in $\mathbb{Z}_q$;
- e is *admissible*, that is
  - e is efficiently computable for any pair in $\mathbb{G}_1 \times \mathbb{G}_2$;
  - e is non-degenerate: the map does not send all pairs in $\mathbb{G}_1 \times \mathbb{G}_2$ to the identity $1_{\mathbb{G}_T}$ in $\mathbb{G}_T$ (i.e., $e(g_1, g_2) \neq 1_{\mathbb{G}_T}$, when $g_1 \neq 1_{\mathbb{G}_1}$ and $g_2 \neq 1_{\mathbb{G}_2}$).

The function e is simply called *bilinear map*, or *pairing*. When $\mathbb{G}_2 = \mathbb{G}_1$ we talk about *symmetric bilinear group*. In this case, we identify the bilinear group with $(q, \mathbb{G}_1, \mathbb{G}_T, e)$.

We recall that, since q is a prime, every element in $\mathbb{G}_i$ (excluding $1_{\mathbb{G}_i}$) is a generator of $\mathbb{G}_i$, for $i = 1, 2, T$.

Remark 4. It is also possible to consider the groups $\mathbb{G}_1$ and $\mathbb{G}_2$ as additive cyclic groups. In this case, the bilinearity property corresponds to $e(aP, bQ) = e(P, Q)^{ab}$,

for $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. For the assumptions presented in the following, there is an equivalent one with $\mathbb{G}_1$ and $\mathbb{G}_2$ additive groups. For the sake of simplicity, we describe here only the assumptions in the multiplicative form.

Explicit constructions of admissible symmetric bilinear maps have been presented, see, e.g., [40] where concrete examples of groups $\mathbb{G}_1, \mathbb{G}_T$ are given, together with an admissible bilinear map between them. Unfortunately, computing pairings incurs a high computational cost and represents the bottleneck of using pairings in actual protocols. In general, $\mathbb{G}_1$ is an abelian variety over some fields. For instance, $\mathbb{G}_1$ is typically the group of points on an elliptic curve over a finite field. The choice of the elliptic curve, e.g., a supersingular curve or an MNT curve [135], has performance implications. Whereas $\mathbb{G}_T$ usually is a finite field. The most common examples of bilinear maps are the (modified) Weil pairing and Tate pairing of supersingular elliptic curves. These maps are non-trivial to compute, and the known algorithms used to compute them, e.g., the Miller's algorithm [134], and refinements thereof [33], are computationally expensive. For an overview of elliptic curves, we refer the interested reader to [167, 148].

Notation. In the following, g and h denote random generators of $\mathbb{G}_1$ and $\mathbb{G}_2$, respectively.

We are ready to introduce all the necessary assumptions.

Assumption (CDH)**.** *The Computational Diffie-Hellman problem in $\mathbb{G}_1$ is to compute the element g^{ab} given the tuple $\left[g, g^a, g^b \right]$ for random $a, b \in \mathbb{Z}_q$. The CDH assumption holds if the CDH problem is hard to solve.*

Assumption (DDH)**.** *The Decisional Diffie-Hellman problem in $\mathbb{G}_1$ is, given the tuple $\left[g, g^a, g^b \right]$, to distinguish between g^{ab} and g^c, where a, b, c are random in $\mathbb{Z}_q$. The DDH assumption holds if solving the DDH problem is difficult.*

In this section, k denotes a positive natural number.

Assumption (PDDH)**.** *Let $k \geq 2$. The k-Party Decisional Diffie-Hellman problem in $\mathbb{G}_1$ is, given the tuple $[g, g^{a_1}, \ldots, g^{a_k}]$, to distinguish between $g^{a_1 \cdots a_k}$ and g^b, where $a_1, \ldots, a_k, b$ are random in $\mathbb{Z}_q$. The k-PDDH assumption holds if solving the k-PDDH problem is hard.*

Note that 2-PDDH assumption is equal to the DDH assumption. The 3-PDDH is first introduced in [46].

Many cryptographic schemes are based on the *discrete logarithm problem*, that is, given $g_1, g_2 \in \mathbb{G}$ for a finite group $\mathbb{G}$, where $g_2 = g_1^a$ for some $a \in \mathbb{Z}_{|G|}$, to find a. Bilinear maps can provide a connection between the discrete logarithm problems of different groups. Moreover, the DDH problem is affected by these maps. The following result is well-known, see for instance [40].

Lemma 3.2. *If there exists an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, then*
   1. *the DDH problem in $\mathbb{G}_1$ is easy to solve;*
   2. *the discrete logarithm problem in $\mathbb{G}_1$ can be reduced to the discrete logarithm problem in $\mathbb{G}_T$ (MOV reduction [133]).*

Proof.
   1. Given $\left[g, g^a, g^b \right]$ and a fourth element g^c, to verify whether c is a random element in $\mathbb{Z}_q$ or $c = ab$, it is sufficient to compute and compare $e(g^a, g^b) = e(g^{ab}, g)$ and $e(g^c, g)$.

2. Given $[g, g^a]$ in $\mathbb{G}_1$, one can compute $e(g, g^a) = e(g, g)^a$. Since $e(g, g)$ is not the identity of $\mathbb{G}_T$ due to the non-degeneracy of e, if an adversary can solve the discrete logarithm problem in $\mathbb{G}_T$, it is able to find a.

$\square$

Note that even assuming the existence of a bilinear map from $\mathbb{G}_1$ to $\mathbb{G}_T$, the CDH problem in $\mathbb{G}_1$ can still be hard.

Since the DDH problem can be easily solved with a bilinear map, several variants of this assumption have been proposed, and many cryptosystems base their security on these variants.

Assumption (XDH and SXDH). *Let $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ be an asymmetric bilinear group such that the CDH problem is intractable in both $\mathbb{G}_1$ and $\mathbb{G}_2$. The external Diffie-Hellman (XDH) assumption states that the DDH problem is intractable in $\mathbb{G}_1$. If the DDH problem is also intractable in $\mathbb{G}_2$, we have the symmetric external Diffie-Hellman (SXDH) assumption.*

Remark 5. In practice, to our knowledge, there is no group in which the CDH problem is intractable, but the DDH problem is not.

Assumption (BDH). *The (symmetric and computational) Bilinear Diffie-Hellman problem for $(q, \mathbb{G}_1, \mathbb{G}_T, e)$ is to compute $e(g, g)^{abc}$ given $[g, g^a, g^b, g^c]$ for random $a, b, c \in \mathbb{Z}_q$. The BDH assumption holds if the BDH problem is challenging to solve.*

Remark 6. The BDH problem in $(q, \mathbb{G}_1, \mathbb{G}_T, e)$ is no harder than the CDH problem in $\mathbb{G}_1$ or $\mathbb{G}_T$. That is, an algorithm that can solve the CDH problem in $\mathbb{G}_1$ or $\mathbb{G}_T$ is sufficient for solving BDH in $(q, \mathbb{G}_1, \mathbb{G}_T, e)$.

Assumption (DBDH). *Consider now $a, b, c, x \in \mathbb{Z}_q$ taken at random. The Decisional Bilinear Diffie-Hellman assumption in $(q, \mathbb{G}_1, \mathbb{G}_T, e)$ states that, given the tuple $[g, g^a, g^b, g^c]$, it is hard to distinguish $e(g, g)^{abc}$ from a random element of $\mathbb{G}_T$.*

In [53], we find the DBDH problem for $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ in its asymmetric version: to distinguish between $e(g, h)^{abc}$ and a random element in $\mathbb{G}_T$, given a tuple $[g, g^a, g^c, h, h^a, h^b]$ for random $a, b, c \in \mathbb{Z}_q$ and g, h in $\mathbb{G}_1, \mathbb{G}_2$, respectively.

In [160], the *Decisional Modified Bilinear Diffie-Hellman* assumption is described.

Assumption (DMBDH). *The Decisional MBDH assumption in $(q, \mathbb{G}_1, \mathbb{G}_T, e)$ holds if, given $[g, g^a, g^b, g^c]$, it is hard to distinguish $e(g, g)^{\frac{ab}{c}}$ from $e(g, g)^z$, for random $a, b, c, z \in \mathbb{Z}_q$.*

Another modification of the DBDH assumption is the *Decisional Bilinear Diffie-Hellman Inversion* assumption that we present below together with the corresponding computational version.

Assumption (DBDHI). *The k-BDHI problem for $(q, \mathbb{G}_1, \mathbb{G}_T, e)$ is defined as follows: given the tuple $[g, g^x, g^{x^2}, \ldots, g^{x^k}]$ for random $x \in \mathbb{Z}_q$, to compute $e(g, g)^{1/x}$. The BDHI assumption holds if this problem is intractable. The decisional k-BDHI problem requires then to distinguish $e(g, g)^{1/x}$ from a random element in $\mathbb{G}_T$. The decisional k-BDHI assumption holds if this problem is challenging.*

The following result is well-known (see for example [35]), but for the sake of completeness, we present proof.

Lemma 3.3. *The 1-BDHI assumption is equivalent to the standard BDH assumption.*

Proof. Let $\mathcal{A}$ be an adversary. Assume that $\mathcal{A}$ can solve the BDH problem and it is given $[g, g^x]$. $\mathcal{A}$ sets $t = g^x$ and $a = b = c = \frac{1}{x}$ $(t^a = g)$. Solving the BDH problem over $[t, t^a, t^b, t^c]$ determines $e(t, t)^{abc}$. Since $e(t, t)^{abc} = e(g^x, g^x)^{\frac{1}{x^3}} = e(g, g)^{\frac{1}{x}}$, the adversary can solve the 1-BDHI problem.

On the other hand, assume now that $\mathcal{A}$ can solve the 1-BDHI problem and takes in input $[g, g^a, g^b, g^c]$. For $d \in \mathbb{Z}_q$, if $\mathcal{A}$ sets $t = g^d$ then $[g, g^d] = \left[t, t^{\frac{1}{d}}\right]$ and it can compute $e(t, t)^d = e(g, g)^{d^3}$. Since $\gcd(6, q) = 1$ and

$$abc = \frac{1}{6} \left[(a + b + c)^3 - (a + b)^3 - (b + c)^3 - (a + c)^3 + a^3 + b^3 + c^3 \right],$$

$\mathcal{A}$ can compute the term $e(g, g)^{abc}$ from the terms $e(g, g)^d$, with $d \in \{a, b, c, a + b, a + c, b + c, a + b + c\}$. It follows that $\mathcal{A}$ can solve the BDH problem, as well. $\square$

Remark 7. It is not known whether the k-BDHI assumption, for $k \geq 2$, is equivalent to BDH. Instead, when considering the decisional formulation of the mentioned assumptions, the decisional BDH assumption is no stronger than the decisional 1-BDHI assumption. Indeed, the first implication in the previous proof can be modified using the decisional formulation without affecting its validity.

Assumption (DBDHE). *The Decisional k-Bilinear Diffie-Hellman Exponent problem for $(q, \mathbb{G}_1, \mathbb{G}_T, e)$ is defined as follows: given a tuple*

$$\left[g_1, g_1^a, g_1^{a^2}, \ldots, g_1^{a^k}, g_1^{a^{k+2}}, \ldots, g_1^{a^{2k}}, g_2 \right],$$

where $a \in \mathbb{Z}_q$ and $g_1, g_2 \in \mathbb{G}_1$ are chosen at random, to distinguish $e(g_1, g_2)^{a^{k+1}}$ from a random element in $\mathbb{G}_T$. The decisional k-BDHE assumption holds if the decisional k-BDHE problem is difficult to solve.

The following assumptions are both modifications of the DBDHE assumption introduced in [179] and [92], respectively.

Assumption (DPBDHE). *The Decisional Parallel k-Bilinear Diffie-Hellman Exponent problem for $(q, \mathbb{G}_1, \mathbb{G}_T, e)$ is defined as follows. Consider $a, s, b_1, \ldots, b_k \in \mathbb{Z}_q$ chosen at random. The problem consists in, given*

$$\Big[g, g^s, g^a, \ldots, g^{a^k}, g^{a^{k+2}}, \ldots, g^{a^{2k}}$$
$$\forall\, 1 \leq j \leq k, \; g^{sb_j}, g^{a/b_j}, \ldots, g^{a^k/b_j}, g^{a^{k+2}/b_j}, \ldots, g^{a^{2k}/b_j},$$
$$\forall\, 1 \leq i, j \leq k, i \neq j, \; g^{asb_i/b_j}, \ldots, g^{a^k sb_i/b_j} \Big],$$

distinguishing $e(g, g)^{a^{k+1}s} \in \mathbb{G}_T$ from a random element in $\mathbb{G}_T$. The decisional k-PBDHE assumption holds if the decisional k-PBDHE problem is hard to solve.

Assumption (DABDHE). *The Decisional k-Augmented Bilinear Diffie-Hellman Exponent problem for $(q, \mathbb{G}_1, \mathbb{G}_T, e)$ consists in, giving the tuple*

$$\left[g_1, g_1^a, g_1^{a^2}, \ldots, g_1^{a^k}, g_1^{a^{k+2}}, \ldots, g_1^{a^{2k}}, g_2, g_2^{a^{k+2}} \right],$$

distinguishing $e(g_1, g_2)^{a^{k+1}}$ from a random element of $\mathbb{G}_T$, where $a \in \mathbb{Z}_q$ and $g_1, g_2 \in \mathbb{G}_1$ are chosen at random. The decisional k-ABDHE assumption holds

if the DABDHE problem is difficult to solve. Gentry in [92] *also presents a truncated version of this problem, where the terms* $g_1^{a^{k+2}}, \ldots, g_1^{a^{2k}}$ *are omitted from the given tuple.*

We now consider other assumptions not directly based on the Diffie-Hellman problem.

Assumption (DLIN). *As presented in* [38], *the Decisional Linear assumption for* $\mathbb{G}_1$ *states that, given the tuple* $\left[g, g^a, g^b, g^{ac}, g^{bd}\right]$ *for random* $a, b, c, d \in \mathbb{Z}_q$, *it is hard to distinguish* g^{c+d} *from a random element of* $\mathbb{G}_1$.

The following claim is well-known, see for example [53], but for sake of completeness we present a proof.

Lemma 3.4. *DLIN assumption for* $\mathbb{G}_1$ *implies DBDH assumption for* $(q, \mathbb{G}_1, \mathbb{G}_T, e)$.

Proof. Let $\mathcal{A}$ be an adversary and assume that $\mathcal{A}$ can solve DBDH. Given the tuple $\left[g, g^a, g^b, g^{ac}, g^{bd}\right]$ the goal is to decide whether an element g^t is g^{c+d} or a random element in $\mathbb{G}_1$. The adversary first computes $e(g^b, g^{ac})e(g^a, g^{bd}) = e(g, g)^{ab(c+d)}$, then $\mathcal{A}$ considers the DBDH problem on input $\left[g, g^a, g^b, g^t\right]$. Since $\mathcal{A}$ can distinguish whether $e(g, g)^{ab(c+d)}$ is $e(g, g)^{abt}$ or not, then $\mathcal{A}$ can distinguish whether $t = c + d$ or not. $\qquad\square$

Notice that this proof cannot be directly extended to the computational cases.

In [53], it is presented an asymmetric version of DLIN assumption for the bilinear group $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, where the given tuple includes also the elements h, h^a, h^b. Note that the implication showed in Lemma 3.4 can be extended similarly to the asymmetric version of the assumptions.

One variant of the DLIN assumption is the *External Decisional Linear* assumption. Basically, it extends the DLIN problem to an asymmetric bilinear group assuming its hardness on both groups.

Assumption (XDLIN). *Given the tuple* $\left[g, g^a, g^b, g^{ac}, g^{bd}, h, h^a, h^b, h^{ac}, h^{bd}\right]$, *for random* $a, b, c, d \in \mathbb{Z}_q$, *the external DLIN assumption in* $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ *states that it is difficult to distinguish* g^{c+d} *from a random element of* $\mathbb{G}_1$ *as well as it is difficult to distinguish* h^{c+d} *from a random element of* $\mathbb{G}_2$.

3.1.1. **Multilinear maps.**

Definition 3.5. A *k-linear map* is a tuple $(q, \mathbb{G}_1, \ldots, \mathbb{G}_k, \{e_{ij} : i, j \geq 1, i + j \leq k\})$ such that:

- $e_{ij} : \mathbb{G}_i \times \mathbb{G}_j \to \mathbb{G}_{i+j}$,
- each $(q, \mathbb{G}_i, \mathbb{G}_j, \mathbb{G}_{i+j}, e_{ij})$ is a bilinear group.

Let g_i be a generator of group $\mathbb{G}_i$ and let $g = g_1$.

The complexity of many protocols can be reduced if cryptographic multilinear maps are used; see, for instance, [49]. In practice, multilinear maps are challenging to construct, as mentioned in [101]. Some candidates are presented in [87, 72, 94], but these multilinear maps suffer from a class of attacks known as "zeroizing" attacks [67], which render them unusable for many applications. To our knowledge, there is only one currently published multilinear map that has not been attacked [131].

Assumption (MDHE). *Consider $c_1, \ldots, c_k \in \mathbb{Z}_q$ chosen at random and let $\ell \geq 2$ be a natural number. The (k, ℓ)-Multilinear Diffie-Hellman Exponent problem for $(q, \mathbb{G}_1, \ldots, \mathbb{G}_k, \{e_{ij}\})$, is, given the following tuple*

$$\left[g^{c_1}, \ldots, g^{c_1^\ell}, g^{c_1^{\ell+2}}, \ldots, g^{c_1^{2\ell}}, g^{c_2}, \ldots, g^{c_k} \right],$$

to distinguish between $g_k^{c_1^{\ell+1} \prod_{2 \leq i \leq k} c_i}$ and a random element of $\mathbb{G}_k$. The MDHE assumption holds if the MDHE problem is hard to solve.

Note that for $k = 2$ this corresponds to the BDHE problem.

3.1.2. **Bilinear groups of composite order.** We now consider cyclic groups of composite order n. In particular, we consider now *symmetric* bilinear groups $(n, \mathbb{G}_1, \mathbb{G}_T, e)$ as in Definition 3.1 but with order $n = pq$, where p and q are two distinct primes. In this case, the groups are still cyclic but not every element is a generator. If one knows the factorisation of n, namely p and q, then the following problems lose interest. For this reason, the adversary is supposed not to get the primes p and q, and we have to assume the hardness of finding a non-trivial factorisation of n.

As noted in [110], using composite order groups typically gives a simpler scheme; however, since the group sizes are larger, group operations are less efficient.

Recall that for any finite group $\mathbb{G}$ of order n and for any divisor m of n, there exists a unique subgroup of $\mathbb{G}$ of order m.

Notation. In the following, $\mathbb{G}_p$ and $\mathbb{G}_q$ denote the subgroups of $\mathbb{G}_1$ of order p and q, respectively. Moreover, g_p and g_q denote random generators of $\mathbb{G}_p$ and $\mathbb{G}_q$, respectively.

In this context, the BDH assumption takes the following form.

Assumption (DcBDH). *The Decisional composite Bilinear Diffie-Hellman assumption for $(n, \mathbb{G}_1, \mathbb{G}_T, e)$ states that, given $\left[g_q, g_p, g_p^a, g_p^b, g_p^c \right]$, for $a, b, c \in \mathbb{Z}_p$ all chosen at random, it is difficult to distinguish between $e(g_p, g_p)^{abc}$ and a random element in $\mathbb{G}_T$.*

Assumption (Dc3DH). *The Decisional composite 3-party Diffie-Hellman assumption for $(n, \mathbb{G}_1, \mathbb{G}_T, e)$ states that, given the tuple $\left[g_q, g_p, g_p^a, g_p^b, g_p^{ab} R_1, g_p^{abc} R_2 \right]$, for $a, b, c \in \mathbb{Z}_p$, and $R_1, R_2, R_3 \in \mathbb{G}_q$, all chosen at random, it is hard to distinguish between $g_p^c R_3$ and a random element in $\mathbb{G}_1$.*

Notice that by knowing p and q and an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$, the assumption is, as we show now, false. Recall that any element $R \in \mathbb{G}_q$ satisfies $R^q = 1_{\mathbb{G}_1}$, where $1_{\mathbb{G}_1}$ stands for the identity element of $\mathbb{G}_1$. Hence, given $\left[g_q, g_p, g_p^a, g_p^b, g_p^{ab} R_1, g_p^{abc} R_2 \right]$ and another element $Z \in \mathbb{G}_1$, we only need to verify whether $e((g_p^{ab} R_1)^q, Z^q)$ equals $e((g_p^{abc} R_2)^q, g_p^q)$. Indeed if $Z = g_p^c R_3$ then $e((g_p^{ab} R_1)^q, (g_p^c R_3)^q) = e(g_p^{abq}, g_p^{cq}) = e(g_p, g_p)^{abcq^2}$ and $e((g_p^{abc} R_2)^q, g_p^q) = e(g_p, g_p)^{abcq^2}$.

We further consider groups of order n, where n is a product of three distinct primes, namely $n = pqr$, and a symmetric bilinear group $(n, \mathbb{G}_1, \mathbb{G}_T, e)$.

Notation. In the following, $\mathbb{G}_p, \mathbb{G}_q$, and $\mathbb{G}_r$ denote the subgroups of $\mathbb{G}_1$ of order p, q and r, respectively. Moreover, g_p, g_q, and g_r denote, respectively, their generators.

The following assumption has been introduced in [116].

Assumption (SD3). *The Subgroup decision problem for three primes for the bilinear group $(n, \mathbb{G}_1, \mathbb{G}_T, e)$ asks, given the tuple $[g_p, g_r]$, to decide whether an element of $\mathbb{G}_1$ is an element of the form $g_p^a g_q^b \in \mathbb{G}_{pq}$ or of the form $g_p^c \in \mathbb{G}_p$, where $a, c \in \mathbb{Z}_p$, $b \in \mathbb{Z}_q$, and $\mathbb{G}_{pq}$ is the subgroup of order pq in $\mathbb{G}_1$. In other words, the SD3 problem asks to distinguish whether a given element of $\mathbb{G}_{pq}$ is an element of $\mathbb{G}_p$ or not. The SD3 assumption holds if the SD3 problem is hard to solve.*

The following two assumptions are introduced in [110].

Assumption (D3c3DH). *For $(n, \mathbb{G}_1, \mathbb{G}_T, e)$, choose random $Q_1, Q_2, Q_3 \in \mathbb{G}_q$, random $R_1, R_2, R_3 \in \mathbb{G}_r$ and random $a, b, s \in \mathbb{Z}_p$. Given*

$$\left[g_p, g_r, g_q R_1, g_p^b, g_p^{b^2}, g_p^a g_q, g_p^{ab} Q_1, g_p^s, g_p^{bs} Q_2 R_2 \right],$$

it is supposed to be hard to distinguish between $g_p^{b^2 s} R_3$ and $g_p^{b^2 s} Q_3 R_3$. We name this assumption the Decisional 3-composite 3-party Diffie-Hellman assumption.

As for the SD3 assumption, knowing q and pr, a non-trivial factorisation of n, makes the hypothesis trivial. Indeed, the problem of distinguishing whether an element $T \in \mathbb{G}_1$ is of the form $g_p^{b^2 s} R_3$ or $g_p^{b^2 s} Q_3 R_3$ can be solved by computing T^{pr}. Indeed, $(g_p^{b^2 s} R_3)^{pr} = 1_{\mathbb{G}_1}$ and $(g_p^{b^2 s} Q_3 R_3)^{pr} = Q_3^{pr}$. Moreover, note that if the element $g^{b^2 s}$ is somehow known, then the D3c3DH problem can be trivially reduced to the SD3 problem.

Assumption (D3c3BDH). *The Decisional 3-composite 3-party Bilinear Diffie-Hellman assumption for $(n, \mathbb{G}_1, \mathbb{G}_T, e)$ states that, chosen at random $h \in \mathbb{G}_p$, $Q_1, Q_2 \in \mathbb{G}_q$ and $s, t \in \mathbb{Z}_q$, given*

$$\left[g_p, g_q, g_r, h, g_p^s, h^s Q_1, g_p^t Q_2, e(g_p, h)^t \right],$$

it is hard to distinguish between $e(g_p, h)^{st}$ and a random element in $\mathbb{G}_T$.

3.2. MATRIX DIFFIE-HELLMAN ASSUMPTIONS. Let $q \in \mathbb{N}$ be a prime and $\mathbb{G}$ be a multiplicative group of order q. Denote by g a generator of $\mathbb{G}$. For an element $a \in \mathbb{Z}_q$, we define $[a] = g^a$ as the implicit representation of a in $\mathbb{G}$. More generally, for a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n \times m}$, we define $[\mathbf{A}]$ as the implicit representation of $\mathbf{A}$ in $\mathbb{G}$, that is $[\mathbf{A}] = (g^{a_{ij}})$.

Definition 3.6. Let $\ell, k \in \mathbb{N}$, with $\ell > k$. We call $\mathcal{D}_{\ell, k}$ a *matrix distribution* if its values are matrices in $\mathbb{Z}_q^{\ell \times k}$ of full rank k.

We assume that matrices can be obtain from $\mathcal{D}_{\ell, k}$ in polynomial time, with overwhelming probability.

Assumption (MDDH). *The $\mathcal{D}_{\ell, k}$-Matrix Decisional Diffie-Hellman assumption for $\mathbb{G}$ states that, given $[\mathbf{A}]$, where $\mathbf{A}$ is drawn from a matrix distribution $\mathcal{D}_{\ell, k}$, it is hard to distinguish between $[\mathbf{A}\mathbf{v}]$ and $[\mathbf{u}]$, with $\mathbf{v} \in (\mathbb{Z}_q)^k$ and $\mathbf{u} \in (\mathbb{Z}_q)^\ell$ chosen at random.*

The MDDH assumption was introduced in [83]. The following is its bilateral version, defined for asymmetric bilinear groups $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$. Let $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n \times m}$ be a matrix. Then, $[\mathbf{A}]_i$ denotes the implicit representation of $\mathbf{A}$ in $\mathbb{G}_i$, for $i = 1, 2$.

Assumption (BMDDH). *The Bilateral $\mathcal{D}_{\ell,k}$-Matrix Decisional Diffie-Hellman assumption for $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$ states that, given $[[\mathbf{A}]_1, [\mathbf{A}]_2]$, where $\mathbf{A}$ is drawn from a matrix distribution $\mathcal{D}_{\ell,k}$, it is hard to distinguish between the two tuples $[[\mathbf{Av}]_1, [\mathbf{Av}]_2]$ and $[[\mathbf{u}]_1, [\mathbf{u}]_2]$, with $\mathbf{v} \in (\mathbb{Z}_q)^k$ and $\mathbf{u} \in (\mathbb{Z}_q)^\ell$ chosen at random.*

3.3. Dual-pairing vector space (DPVS). The DPVS [140, 141] is defined by the tuple $(q, \mathbb{V}, \mathbb{W}, \mathbb{G}_T, \mathbb{A}, \mathbb{B}, \tilde{e})$, which is directly constructed from the bilinear group $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e)$, where q is a prime. Assume $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ are multiplicative cyclic groups of order q, and let g, h be generators of $\mathbb{G}_1, \mathbb{G}_2$, respectively. In detail, $\mathbb{V} = (\mathbb{G}_1)^n$ and $\mathbb{W} = (\mathbb{G}_2)^n$ are n-dimensional vector spaces over $\mathbb{Z}_q$, where $\mathbf{x} = (g^{x_1}, \ldots, g^{x_n}) \in \mathbb{V}$ and $\mathbf{y} = (h^{y_1}, \ldots, h^{y_n}) \in \mathbb{W}$, with $x_i, y_i \in \mathbb{Z}_q$. Given $\mathbf{x}, \mathbf{z} \in \mathbb{V}$, the sum $\mathbf{x} + \mathbf{z}$, required in the definition of a vector space, is here replaced by a component-wise multiplication, that is, $\mathbf{x} + \mathbf{z} = \left(g^{(x_1+z_1)}, \ldots, g^{(x_n+z_n)}\right)$, and, given $a \in \mathbb{Z}_q$, the scalar multiplication is defined as $a\mathbf{x} = (g^{ax_1}, \ldots, g^{ax_n})$. The operations on $\mathbb{W}$ are defined in a similar way. $\mathbb{A}$ and $\mathbb{B}$ are canonical bases for $\mathbb{V}$ and $\mathbb{W}$, respectively. That is, $\mathbb{A} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ where $\mathbf{e}_1 = (g, 1_{\mathbb{G}_1}, \ldots, 1_{\mathbb{G}_1})$, $\mathbf{e}_2 = (1_{\mathbb{G}_1}, g, 1_{\mathbb{G}_1}, \ldots, 1_{\mathbb{G}_1})$, $\ldots$, $\mathbf{e}_n = (1_{\mathbb{G}_1}, \ldots, 1_{\mathbb{G}_1}, g)$, and $\mathbb{B}$ is defined similarly. Finally, $\tilde{e} : \mathbb{V} \times \mathbb{W} \to \mathbb{G}_T$ is a pairing defined by $\tilde{e}(\mathbf{x}, \mathbf{y}) = \prod_{i=1}^n e(g^{x_i}, h^{y_i}) \in \mathbb{G}_T$.

Three typical constructions are given in [140] and [169]. Related to DPVS, we find the *Decisional Subspace Problem* (DSP).

Assumption (DSP). *Let $n_1, n_2 \in \mathbb{N}$, with $n_2 + 1 < n_1$. The Decisional Subspace Problem $\mathrm{DSP}_{(n_1, n_2)}$ assumption for $(q, \mathbb{V}, \mathbb{W}, \mathbb{G}_T, \mathbb{A}, \mathbb{B}, \tilde{e})$ states that, given a base $\mathbb{A}_1 = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_n\}$ of $\mathbb{V}$, it is hard to distinguish $\boldsymbol{v} = v_{n_2+1} \boldsymbol{a}_{n_2+1} + \cdots + v_{n_1} \boldsymbol{a}_{n_1}$ from $\boldsymbol{u} = v_1 \boldsymbol{a}_1 + \cdots + v_{n_1} \boldsymbol{a}_{n_1}$, where $v_1, \ldots, v_{n_1}$ are chosen at random in $\mathbb{Z}_q$.*

In [140], two variants of the DSP assumption are introduced: *Decisional Subspace Problem with Relevant Dual Vector Tuples* (RDSP) and *Decisional Subspace Problem with Irrelevant Dual Vector Tuples* (IDSP). Since a complete description of these two variants is rather long and quite technical, we refer the interested reader to [141, Chapter 3]. Moreover, the authors show that DSP is intractable if the generalised DDH or DLIN problem is intractable.

3.4. Learning with errors (LWE). The LWE problem was introduced by Regev [157], who showed that solving it on average is as challenging as solving, with a quantum algorithm, several standard lattice problems in the worst case.

For positive $\ell, n, m \in \mathbb{N}$, with $\ell \geq 2$, and an error distribution χ over $\mathbb{Z}_\ell$, the *(decisional) Learning With Errors* problem is to distinguish between the following pairs of distributions:

$$\{A, As + x\} \text{ and } \{A, u\}$$

where $A \in \mathbb{Z}_\ell^{n \times m}$, $s \in \mathbb{Z}_\ell^n$, $x \in \chi^m$ and $u \in \mathbb{Z}_\ell^m$ are all chosen at random.

3.5. Multivariate quadratic polynomial (MQ) problem. The *Multivariate Quadratic polynomial* problem consists in solving systems of multivariate quadratic equations over finite fields. In detail, denote by $\mathbb{F}_r$ the finite field with r elements, where r is a prime power. Given a system of multivariate polynomials $\{p_1(x_1, \ldots, x_n), \ldots, p_k(x_1, \ldots, x_n)\}$ of degree 2 over $\mathbb{F}_r$, the (computational) MQ problem requires to find a solution $\mathbf{x} \in (\mathbb{F}_r)^n$ such that $p_1(\mathbf{x}) = \cdots = p_k(\mathbf{x}) = 0$. The MQ problem is proved to be NP-complete [86, 152], even for polynomials of degree 2 over $\mathbb{F}_2$. The relevance, in cryptography, of the MQ problem, relies on its quantum resistance.

3.6. NUMBER THEORY ASSUMPTIONS. We mention also two assumptions belonging to the field of number theory.

Definition 3.7. Given three integers a, k and N, a is a *k-th residue* modulo N if there exists an integer b such that $a \equiv b^k \bmod N$. If k is equal to 2, then a is called *quadratic residue* modulo N.

Assumption (QR). *The Quadratic Residuosity problem is to decide, given two integers a and N, whether a is a quadratic residue modulo N or not. The QR assumption holds if the QR problem is intractable.*

Notice that, for an odd prime p, it holds

$$a^{\frac{p-1}{2}} \bmod p = \begin{cases} 0 & \text{if } a \equiv 0 \bmod p, \\ 1 & \text{if } a \text{ is a quadratic residue,} \\ -1 & \text{otherwise.} \end{cases}$$

Moreover, for a prime factor p of N, a is a quadratic residue modulo N only if a is a quadratic residue modulo p. Therefore, in the formulation of the QR problem, we assume that no non-trivial factorisation of N is known.

Assumption (DCR). *Let p, q, p', q' be distinct odd primes with $p = 2p' + 1$ and $q = 2q' + 1$, and such that p' and q' have the same bit length. Let $N = pq$. The Paillier's Decisional Composite Residuosity (DCR) assumption states that, given only N, it is hard to decide whether an element of $\mathbb{Z}_{N^2}$ is an N-th residue modulo N^2 or not.*

4. SECURITY

The idea of security for an FE scheme is that even collusion of secret keys (functional decryption keys) for different functionalities does not reveal anything more about a plaintext than what each secret key allows a user to learn. Two different models of security for an FE scheme have been used mainly: *indistinguishability-based security* and *simulation-based security*, shortly IND-based and SIM-based security. The former requires that an adversary cannot distinguish between ciphertexts of any two messages m_0, m_1 of its choosing, with access to some secret keys sk_f of functions f such that $f(m_0) = f(m_1)$. By contrast, the latter requires that the adversary's view can be simulated by a simulator, given only access to secret keys and functions evaluated on the corresponding messages. SIM-based security has higher security strength than IND-based security. Indeed, SIM-based security implies IND-based security, and there exist IND-based secure FE schemes for certain functionalities which are not able to be proved secure under SIM-based security, see the example in Subsection 4.2.

In the following, we present in more detail the aforementioned security models and other related notions.

4.1. INDISTINGUISHABILITY-BASED SECURITY. In this security game, an adversary $\mathcal{A}$ receives the public key of the encryption scheme, and then it can request functional decryption keys for functions f of its choice. $\mathcal{A}$ also sends two messages, m_0 and m_1, to the challenger, which samples a random bit b and sends back encryption of the message m_b. We require that the functional decryption keys, obtained by the adversary, are associated with functions f that do not distinguish the two messages, for which $f(m_0) = f(m_1)$. The system is IND-based secure if the probability that

the adversary guesses which bit b was used is close[1] to the probability of a random guess, corresponding to $1/2$.

When the adversary can choose the challenge messages adaptively, we refer to *adaptive security* (also called *full security*). In this setting, the game for an adversary $\mathcal{A}$ can be described as follows.

- **Setup**: run $\texttt{Setup}(1^\lambda) \to (\mathrm{pp}, \mathrm{mk})$ and give pp to $\mathcal{A}$.
- **Query1**: $\mathcal{A}$ adaptively submits a polynomial number of queries for $f_i \in \mathcal{F}$, with $i = 1, 2, \ldots, n$, and it is given $\texttt{KeyGen}(\mathrm{mk}, f_i) \to \mathrm{sk}_{f_i}$.
- **Challenge**: $\mathcal{A}$ submits two messages $m_0, m_1 \in X$ satisfying

(1) $$f_i(m_0) = f_i(m_1) \text{ for all } i = 1, \ldots, n,$$

  and it is given $\texttt{Enc}(\mathrm{pp}, m_b)$.
- **Query2**: $\mathcal{A}$ continues to issue key queries as in **Query1** satisfying (1), and eventually outputs a bit in $\{0, 1\}$.

The adversary wins the game if it guesses correctly the bit b. This notion is sometimes referred as IND-CPA, where CPA stands for chosen-plaintext attack. This definition, taken from [47], is a generalisation of related definitions from [50, 110]. An artificial but beneficial weakening of this security model is the so-called *selective security*, where the adversary is required to choose between m_0 and m_1 beforehand, that is, before obtaining any functional decryption keys or even seeing the public key. Hence, in this security model the **Query1** phase is eliminated and the **Challenge** phase is either right after or right before the **Setup** phase. A transformation from selective to fully secure (IND-based) functional encryption can be found in [21] for some cases. In literature, we can find modifications of this security game, for example, to a chosen-ciphertext one (CCA) as in [36].

4.2. Simulation-based security. Consider the following generalisation of the FE scheme described in [47]. For a key space $K = \{k_1, \ldots, k_t\}$ consider t permutation maps $\sigma_1, \ldots, \sigma_t$ of the plaintext space and the following functionalities $F(k_i, x) = \sigma_i(x)$ for $i = 1, \ldots, t$. Consider now an FE scheme with a trivial encryption algorithm $\texttt{Enc}(\mathrm{pp}, x) = x$ and such that $\texttt{Dec}(\mathrm{sk}_i, x) = \sigma_i(x)$, where sk_i is the secret key corresponding to key $k_i \in K$.

This scheme clearly leaks more information about the plaintext x than needed. However, if we consider an IND-game, the adversary is forced to issue identical challenge messages. Indeed, for every secret key sk_i known by the adversary, we require $\sigma_i(m_0) = \sigma_i(m_1)$. This trivially implies that the scheme is IND-secure. As shown in the example and pointed out by Boneh et al. in [47], IND-based security is vacuous and inadequate for specific functionalities. This indicates that we should opt for simulation-based security whenever possible. In the definition of SIM-based security, an efficient simulator is required to generate the view of the adversary in the security game, only knowing the information that leaks from the encrypted values and corrupted functional decryption keys (possessed by the adversary). This security notion for FE schemes was first given in [146, 47]. In the following, we report in more detail the idea of SIM-based security, as given in [48].

Let $\mathcal{A}$ be a polynomial time adversary that takes as input the public key pp, a set of secret keys $\{\mathrm{sk}_i = \texttt{KeyGen}(\mathrm{mk}, f_i) : 1 \leq i \leq \ell\}$ for functions $f_i \in \mathcal{F}$ of its choice, and a ciphertext $c = \texttt{Enc}(\mathrm{pp}, x)$. Then $\mathcal{A}$ might output some information about the

---

[1]Two probabilities are close if their difference is a negligible function concerning the security parameter.

decryption of c. The system is SIM-based secure if, for every such $\mathcal{A}$ there is another polynomial time algorithm $\mathcal{B}$, called *simulator*, that given pp and $f_1(x), \ldots, f_\ell(x)$, but not given c, is able to output the same information about x that $\mathcal{A}$ outputs. This implies that knowing the ciphertext c does not give any additional information about x, beyond that obtained from $f_1(x), \ldots, f_\ell(x)$.

We refer the reader to [47] for a more formal definition of SIM-based security. We also refer the reader to [90] for the distinction between adaptive and selective SIM-based security.

In [146, 47], it is shown that this security notion is impossible to achieve in many cases. For instance, [47, Theorem 2] states that there are no SIM-based secure IBE schemes in the non-programmable random oracle model (see Subsection 4.4). However, the random oracle model is more promising. In fact, in this model, it is possible to achieve SIM-based security. For example, as exhibited in [47, Theorem 4], given an IND-based secure predicate encryption system with a public index, it is possible to convert the system into a scheme SIM-based secure in the random oracle model.

4.3. FUNCTION PRIVACY. Although the vast majority of research has focused on the privacy of the encrypted messages, it is crucial to offer privacy for the functions for which decryption keys are provided in many realistic scenarios. Indeed, the functions themselves may already leak critical or sensitive information. *Function privacy* was first proposed by Shen, Shi, and Waters in the setting of private-key predicate encryption in [164]. It requires that a secret key sk_f does not reveal anything about the function f. For public-key functional encryption, standard function privacy cannot be generally achieved. Indeed, given a key sk_f, an adversary can generate ciphertexts of messages $x_1, \ldots, x_n$ of its choices, and thus it obtains the values $f(x_1), \ldots, f(x_n)$.

Boneh, Raghunathan, and Segev in [44], and later in [45], address this problem for some public-key predicate encryption schemes. In [44], they construct function-private IBE which implies predicate-private encrypted keyword search. Whereas, in [45], they consider the notion of *subspace-membership encryption*, a generalisation of inner-product encryption that supports subspace-membership predicates. They present a generic construction of a function-private subspace-membership encryption scheme based on any inner-product encryption scheme. Further analysis on HVE can be found in [28].

4.4. RANDOM ORACLE MODEL. The *Random Oracle Model* (ROM) was introduced by Bellare and Rogaway in [29] as an alternative model to analyse the security of certain cryptographic constructions. A *random oracle* is a function $\mathcal{O} : X \to Y$ chosen uniformly at random from the set of all such functions, where Y is supposed to be a finite set. ROM assumes the availability of a random oracle to all parties (adversary, challenger, etc.) playing a role in any game aimed at studying the security of a cryptographic primitive. The introduction of ROM made it possible to prove the security of many different kinds of cryptographic primitives. As truly random functions do not exist in practice, when using these primitives in the real world, a secure hash function plays the role of a random oracle. The heuristic is that secure hash functions are close enough to random oracles in their behavior, so the primitives remain secure even under this substitution.

In ROM, the challenger simulates the random oracle for the adversary in the security game. The challenger can select answers dynamically for the queries that

parties make to the random oracle; we refer to this property as *programmability* of the random oracle. On the other hand, the *non-programmable random oracle model* restricts the challenger such that it can no longer choose return values of the random oracle. This security restriction makes the underlying proofs preferable, as they rely on fewer properties of the random oracle and so can be considered as a step toward getting rid of it. A more detailed description of these models can be found in [85].

ROM is in opposition with the *standard model* in which the adversary is only limited by the amount of time and computation available. A scheme is secure in the standard model if it can be proved secure only using complexity assumptions.

Another model used is the *generic-group model*, which assumes that the properties of the representation of the elements of the group under consideration cannot be exploited. This extends naturally also to bilinear maps.

5. IBE and ABE

Historically, Identity-Based Encryption (IBE) has been the first attempt to construct a functional encryption scheme beyond traditional public-key encryption. IBE schemes have been then generalised into Attribute-Based Encryption (ABE) schemes. Classical IBE and ABE systems are also referred to as predicate encryption systems with a public index or *payload hiding* systems. Indeed, the payload message is hidden, but the index related to it (an identity, a set of attributes, or an access policy) is often in the clear. In the following, we define IBE and ABE systems and briefly introduce some of the known constructions.

5.1. Identity-based encryption. In an IBE scheme we assume that a plaintext to be encrypted is a pair $(\mathrm{ID}, m) \in I \times M$, where ID is the identity and m is the payload message. Secret keys are also associated with an identity ID', and decryption succeeds to recover the payload message if there is a match between the identity associated with the ciphertext and the identity associated with the secret key, that is,

$$F(\mathrm{ID}', (\mathrm{ID}, m)) = \begin{cases} m & \text{if } \mathrm{ID} = \mathrm{ID}', \\ \bot & \text{otherwise.} \end{cases}$$

For example, in an email system, the identity can be the email address and the payload can be the email content. Employing a public-key cryptosystem, it is possible to encrypt a message to any user whose email address is known. Using his identity, the receiver can obtain the corresponding secret key and decrypt all the received messages. The concept of IBE was first thought of by Shamir in 1984 [163] as a way to simplify certificate management in email systems. The first realisations of IBE schemes were given in 2001: the security of these schemes was based on either the BDH or the QR assumption in the random oracle model [40, 71]. In [40], the system is based on bilinear maps between groups (the Weil pairing on elliptic curves is an example of such maps), and it is IND-based secure against an adaptive chosen ciphertext attack. In [71], the system is based on quadratic residues; it is relatively easy to implement, but the ciphertext length is very large (see [42] for an improvement).

Since then, tremendous progress has been made towards obtaining IBE schemes that are secure in the standard model based on pairings as well as on lattices [58, 35, 36, 177, 63, 92, 137, 9, 178, 66]. Different assumptions are used to prove

the security of the cited constructions, such as DBDH, DBDHI, truncated ABDHE, DLIN, and LWE.

Several surveys on IBE schemes have been published during the years. We refer the interested reader to [52, 105, 172].

5.1.1. **Hierarchical IBE.** Some of the mentioned papers also present constructions of HIBE. With Hierarchical IBE (HIBE), we refer to a generalisation of IBE that mirrors an organisational hierarchy. Identities are taken as vectors, and there is a fifth algorithm called `Derive`. A vector of dimension ℓ represents an identity at level ℓ of the hierarchy. Algorithm `Derive` takes as input an identity $\text{ID} = (I_1, \ldots, I_\ell)$ at level ℓ and the private key of the parent identity $\text{ID}' = (I_1, \ldots, I_{\ell-1})$ at level $\ell - 1$. It outputs the private key for an identity ID. So an identity can issue private keys to its descendants' identities, but it cannot decrypt messages intended for other identities. The notion of HIBE was first defined in [107] and constructions in the random oracle model were given in [95] (based on the DBDH assumption). Several works on HIBE schemes followed, and their security is proved in the standard model, see [58, 35, 37, 9, 178, 59]. These schemes are based on different security assumptions such as DBDH, DBDHE, DLIN, and LWE. For a deeper analysis of HIBE schemes, we refer the reader to [74].

5.2. Attribute-based encryption. In many situations, it is required that encrypted sensitive data can be decrypted only by users who have certain credentials or attributes. As an example, consider a company with different branches {Trento, London, Oslo, etc.} where employees are divided into management-levels $\{1, 2, \ldots, 5\}$ and characterised by the years spent working for the company. A sensitive memo about a project in the Italian branch may be encrypted with the following access policies: (branch = Trento `AND` years ≥ 3) `OR` (management-level $= 5$), and only employees with these attributes can read the memo.

To comprehend also these kinds of scenarios, ABE systems are introduced as an extension of IBE. In ABE schemes, sets of attributes or access policies over attributes are used instead of the identities in the encrypted message and the secret key. ABE integrates encryption and access control, and it is ideal for sharing secrets among groups, especially in a cloud environment. Many different ABE schemes with additional features have been proposed during the years.

In the following, we describe some of the main features of ABE schemes. To have a more detailed overview of ABE systems, we refer the reader to [155, 113, 185].

5.2.1. **Threshold-policy access control.** Sets of descriptive attributes (ω, ω') label both the ciphertext and the user's secret key. The decryption is successful if there is a sufficient overlap, say d, between the attribute sets of the ciphertext and the secret key, that is,

$$F(\omega', (\omega, m)) = \begin{cases} m & \text{if } |\omega \cap \omega'| \geq d, \\ \bot & \text{otherwise.} \end{cases}$$

This threshold provides error tolerance for coarse-grained access control schemes, and it is particularly useful to biometric applications where public information, not a secret, is treated as the input. This type of ABE scheme was introduced by Sahai and Waters in 2005 [160] called by the authors *Fuzzy Identity-Based Encryption* scheme. This scheme is based on polynomial interpolation, and it is secure under the decisional MBDH assumption. Since the work of Sahai and Waters, several other

constructions followed; for example, in [61] there is an extension of the Fuzzy-IBE scheme based on the DBDH assumption.

5.2.2. **Key-policy access control.** In Key-Policy ABE (KP-ABE), an access policy ϕ is encoded into a user's secret key, and ciphertext is labeled with a set of descriptive attributes ω. The access structure of the private key specifies which type of ciphertexts the key can decrypt, that is,

$$F(\phi, (\omega, m)) = \begin{cases} m & \text{if } \omega \text{ satisfies } \phi, \\ \bot & \text{otherwise.} \end{cases}$$

In KP-ABE schemes, the data owner has limited control over who can decrypt the data. KP-ABE schemes are suitable for structured organisations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast. The first KP-ABE was presented by Goyal, Pandey, Sahai, and Waters in 2006 [103]. Further results on KP-ABE followed, see for example [23, 142, 100, 41]. KP-ABE schemes are based on different assumptions, such as DBDH, MDHE, DLIN and LWE.

5.2.3. **Ciphertext-policy access control.** In Ciphertext-Policy ABE (CP-ABE), a user's secret key is associated with a list of attributes ω, and a ciphertext specifies an access policy ϕ. A ciphertext can be decrypted by a user if and only if the user's attributes satisfy the ciphertext's access policy, that is,

$$F(\omega, (\phi, m)) = \begin{cases} m & \text{if } \omega \text{ satisfies } \phi, \\ \bot & \text{otherwise.} \end{cases}$$

Hence, the data owner can determine who can decrypt and, if the policy needs to be updated frequently, CP-ABE can be more flexible than KP-ABE. One of the first constructions of CP-ABE appears in [31], which is based on the random oracle assumption. Improvements on CP-ABE schemes can be found in several papers, for example, in [179, 115, 142]. The cited schemes are based on different assumptions, such as the decisional PBDHE, SD3, DLIN.

5.2.4. **Non-monotonic access control.** Usually, KP-ABE and CP-ABE use monotonic access structures, which means that users cannot express the negative attribute to exclude certain users from decryption. The number of attributes could be doubled to introduce the NOT expression: for each original attribute, the system must assign one corresponding negative attribute. This approach is not efficient in the number of attributes to consider. The first non-monotonic attribute-based scheme to reduce the number of negative attributes can be found in [147]. Another non-monotonic system is presented in [23]. The mentioned schemes are based on the DBDH and the DBDHE assumptions.

5.2.5. **Hierarchical ABE.** In Hierarchical ABE (HABE), as for HIBE, the delegation of access privilege is hierarchical. This feature can be helpful when there are many attributes in the system. It relieves the authority (in charge of generating secret keys) from the heavy key management burden. Users are associated with attribute vectors that denote their depth in the hierarchy. Users at a higher level may delegate secret keys to their subordinates. Weng et al.[176] combined HIBE with CP-ABE to achieve HABE. Other HABE schemes can be found in [80, 120].

5.2.6. **Revocable ABE.** The revocation functionality is realised in revocable ABE schemes, where it is possible to revoke malicious users from the system or revoke an expired attribute. For more details, see [108, 114, 96, 17, 73].

5.2.7. **Other features.** Other important features characterise ABE schemes. *Scalability* improves the dynamism of the system: a new user with new attributes is allowed to join the system without restarting. *Key delegation* schemes are characterised by having another algorithm in their definition: $\texttt{Delegate}(\text{sk}_k, \tilde{k}) \rightarrow \text{sk}_{\tilde{k}}$, on input a user's secret key sk_k and a set of attributes $\tilde{k} \subseteq k$, outputs a new user's secret key $\text{sk}_{\tilde{k}}$. Hence a user can create new secret keys for subsets of its attributes set. Both features can be achieved with a hierarchical structure. Another important feature is the *Multi-Authority*. Multi-Authority ABE schemes are described in Subsection 8.6. *Accountability* helps to track misbehaving users by reducing trust assumptions on both authorities and users. For more details on these features, we refer the interested reader to the mentioned surveys on ABE schemes [155, 113, 185].

6. Predicate encryption with private index

As briefly mentioned in Section 2, in a PE scheme a ciphertext is associated with a set of attributes $\mathbf{x}$ (called also *index*), while a decryption secret key is tied to a specific predicate P in some function class $\mathcal{F}$. The secret key sk_P, sometimes called also *token*, correctly decrypts a ciphertext if and only if the associated set of attributes $\mathbf{x}$ satisfies $P(\mathbf{x}) = 1$, that is,

$$F(P, (\mathbf{x}, m)) = \begin{cases} m & \text{if } P(\mathbf{x}) = 1, \\ \bot & \text{otherwise.} \end{cases}$$

Note that both IBE and ABE can be cast in the framework of predication encryption. In particular, IBE schemes can be viewed as predicate encryption for the class of equality tests. A ciphertext in PE hides the message (or payload) m: an adversary holding keys $\text{sk}_{P_1}, \cdots, \text{sk}_{P_\ell}$ learns nothing about a message encrypted using attribute $\mathbf{x}$ only if $P_1(\mathbf{x}) = \ldots = P_\ell(\mathbf{x}) = 0$. This security notion is often referred to as *payload hiding*. If the ciphertext hides also the attributes $\mathbf{x}$, we talk about *attribute hiding* or *private-index PE*. Whereas, IBE and ABE are also called *public-index PE*. Some proposed constructions only hide the attributes underlying each ciphertext when the decryption is not successful. This is referred to as *weakly-hiding the attributes*. Instead, in *fully-hiding* constructions, the only information that leaks is the value of the predicate evaluation, even when the decryption succeeds. In the following, we present the three main classes of private-index PE schemes.

6.1. Anonymous identity-based encryption. With anonymous-IBE, we refer to an IBE scheme in which the ciphertext identity (the index related to the message) is hidden, and one can only determine it by using the corresponding private key (attribute hiding). Most of the IBE schemes presented in Subsection 5.1 are only payload hiding. The IBE system proposed in [40] is inherently anonymous, as noticed by Boyen in [51]. Recall that its security proofs are set in the random oracle model. In the full version of [47], Boneh, Sahai, and Waters show that this system [40] is SIM-based secure (in the random oracle model). In [53], we can find an identity-based cryptosystem that features fully anonymous ciphertexts and hierarchical key-delegation. The proof of security is given in the standard model, based on the DLIN assumption in bilinear groups. The system has small ciphertexts

of size linear in-depth of the hierarchy. Other anonymous IBE constructions, both pairing-based (truncated ABDHE, DBDH, DLIN assumptions) and lattice-based (LWE assumption), can be found in [92, 59, 9, 153, 57]. More recent studies on anonymous IBE can be found in [104, 34, 84, 106, 132, 182].

6.2. Hidden vector encryption. Hidden Vector Encryption (HVE) is a particular case of Predicate Encryption (PE). Boneh and Waters first proposed it in [50] as a subclass of Searchable Encryption systems. Previous Searchable Encryption schemes were proposed in [39] supporting simple equality tests. Let Σ be a finite set of attributes, let $*$ be a special character (not in Σ) and set $\Sigma_* = \Sigma \cup \{*\}$. We refer to $*$ as a *wildcard character*. Often Σ corresponds to the set of binary strings of arbitrary length. For a vector $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_n) \in (\Sigma_*)^n$, a predicate $P_{\boldsymbol{\sigma}}$ over Σ^n is defined as follows: for $\mathbf{x} = (x_1, \ldots, x_n) \in \Sigma^n$

$$P_{\boldsymbol{\sigma}}(\mathbf{x}) = \begin{cases} 1 & \text{if } \forall i \ \sigma_i = x_i \text{ or } \sigma_i = *, \\ 0 & \text{otherwise.} \end{cases}$$

Based on [50], an HVE scheme supporting equality predicates leads to an anonymous IBE scheme where a ciphertext reveals no useful information about the receiver's identity.

In [50], an HVE scheme is constructed based on composite-order bilinear groups. It supports evaluation of conjunctive equality $(x_i = \sigma_i)$, comparison $(x_i \geq \sigma_i)$ and subset predicates $(x_i \in A_i \subseteq \Sigma)$. Additionally, it supports a conjunctive combination of these primitive predicates by extending the size of ciphertexts. The ciphertext size is $\mathcal{O}(n)$ and the token size is $\mathcal{O}(\text{weight}(\boldsymbol{\sigma}))$, where $\text{weight}(\boldsymbol{\sigma}) = \text{weight}((\sigma_1, \ldots, \sigma_n)) = |\{\sigma_i : \sigma_i \neq *\}|$. The scheme is proved selectively IND-based secure under the Dc3DH assumption and the DcBDH assumption, where an adversary has restrictions on the queries it can ask. After the introduction of HVE based on composite-order bilinear groups, several other HVE schemes have been proposed, see e.g. [109, 165, 149, 151, 78, 184, 161]. The mentioned schemes are based on pairings and rely on different assumptions, such as DLIN and DBDH.

6.3. Inner-product predicate encryption. Researchers have tried to expand the function class $\mathcal{P}$ supported by a PE scheme, with the ultimate goal being to handle all polynomial-time predicates. A stepping stone towards this goal is to support the predicated corresponding to inner products over $\mathbb{Z}_N$ (for some large integer N). For a set of attributes $\Sigma = (\mathbb{Z}_N)^n$, we consider the class of predicates $\mathcal{P} = \{P_{\mathbf{x}} \mid \mathbf{x} \in (\mathbb{Z}_N)^n\}$ with

$$P_{\mathbf{x}}(\mathbf{y}) = \begin{cases} 1 & \text{if } \langle \mathbf{x}, \mathbf{y} \rangle = \sum_{i=1}^n x_i \cdot y_i \equiv 0 \bmod N, \\ 0 & \text{otherwise.} \end{cases}$$

Notice that sometimes in literature, these schemes are called IPE (Inner Product Encryption) schemes. This can create confusion with schemes that output the value of the inner product (see Section 7). We then refer to a scheme supporting this class of functionalities as an Inner-Product Predicate Encryption (IP-PE) scheme. In [110], Katz, Sahai, and Waters construct an IP-PE scheme without a random oracle, based on two assumptions in composite-order groups equipped with a bilinear map. The (decisional) assumptions D3c3DH and D3c3BDH, introduced in [110], are shown to hold in the generic-group model, assuming that finding a non-trivial factorisation of the group order is hard. The scheme is proved selective IND-based secure. In the same work, the authors show that any PE scheme supporting inner

product predicates can be used as a building block to construct predicates of more general types. IP-PE implies anonymous-IBE and HVE, and it can construct a PE scheme supporting polynomial evaluation (polynomials of some bounded degree). This allows us to build PE schemes for disjunctions and conjunctions of equality tests and Boolean variables, hence arbitrary CNF and DNF formulas (bounded depth). IP-PE can also be used to construct an (attribute hiding) fuzzy-IBE with an exact threshold policy. We report here some of the mentioned implications, as presented in [110]. Anonymous IBE can be recovered from IP-PE in the following way. To generate secret keys for identity $I \in \mathbb{Z}_N$, set $\mathbf{x} = (1, I)$ and output the secret key for the predicate $P_\mathbf{x}$. To encrypt a message M for identity $J \in \mathbb{Z}_N$, set $\mathbf{y} = (-J, 1)$ and encrypt the message with index $\mathbf{y}$. Then decryption is successful if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, that is, if $I = J$. HVE for predicates over $\Sigma^\ell = (\mathbb{Z}_N)^\ell$ can be recovered from IP-PE by doubling the dimension. Consider the predicate $P_{\boldsymbol{\sigma}}$ described in Subsection 6.2. To generate a secret key corresponding to $P_{\boldsymbol{\sigma}}$, first construct a vector $\mathbf{x} = (x_1, \ldots, x_{2\ell})$ as follows:

$$\text{when } \sigma_i \neq *, \text{ set } x_{2i-1} = 1, \ x_{2i} = \sigma_i,$$
$$\text{when } \sigma_i = *, \text{ set } x_{2i-1} = 0, \ x_{2i} = 0.$$

Then output the secret key for predicate $P_\mathbf{x}$. To encrypt a message M for attribute $\mathbf{z} = (z_1, \ldots, z_\ell)$, choose random $r_1, \ldots, r_\ell \in \mathbb{Z}_N$, construct a vector $\mathbf{y_r} = (y_1, \ldots, y_{2\ell})$ with

$$y_{2i-1} = -r_i \cdot z_i, \ y_{2i} = r_i,$$

and output the corresponding ciphertext. Clearly, if $P_{\boldsymbol{\sigma}}(\mathbf{z}) = 1$ then $\langle \mathbf{x}, \mathbf{y_r} \rangle = 0$ and $P_\mathbf{x}(\mathbf{y_r}) = 1$. On the other side, assuming $\gcd(\sigma_i - z_i, N) = 1$, if $P_{\boldsymbol{\sigma}}(\mathbf{z}) = 0$ then the probability that $\langle \mathbf{x}, \mathbf{y_r} \rangle = 0$ is $1/N$. Finally, polynomial evaluation can be described with IP-PE. Let $a \in \mathbb{Z}_N[x]$ be a polynomial of degree at most d, $a(x) = a_d x^d + \ldots + a_1 x + a_0$, and consider the predicate

$$P_a(x) = \begin{cases} 1 & \text{if } a(x) = 0, \\ 0 & \text{otherwise.} \end{cases}$$

To generate a secret key corresponding to a, set $\mathbf{x} = (a_d, \ldots, a_0)$ and output the key for predicate $P_\mathbf{x}$. To encrypt a message M for the attribute $w \in \mathbb{Z}_N$, set $\mathbf{y} = (w^d \mod N, \ldots, w^0 \mod N)$ and output the corresponding ciphertext. The decryption is then successful if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, that is, if $a(w) = 0$.

The first lattice-based construction of a PE scheme for the inner product is proposed in [11]. The scheme is proved secure (weakly-hiding the attributes) under the LWE assumption. Other constructions of PE schemes supporting inner products can be found in [141, 115, 150, 143, 180]. The above schemes are based on pairings and rely on different assumptions such as RDSP, IDSP, DLIN, and DBDH.

7. Beyond predicate encryption: Inner product encryption

So far, we have only discussed particular kinds of functional encryption where decryption successfully recovers the entire message if the attributes associated with the ciphertext (resp. the functional decryption key) satisfy the access policy embedded in the key (resp. the ciphertext). While this is a fruitful generalisation of traditional public-key encryption, since it permits embedding complex access policies into the encrypted data, it is still an "all-or-nothing" encryption. The *Inner Product Encryption* (IPE), introduced in [2], is the first FE scheme with fine-grained

access to the encrypted data, where decryption recovers partial information about the encrypted data.

In an IPE scheme, a ciphertext $c_{\mathbf{x}}$ is related to a vector $\mathbf{x} = (x_1, \ldots, x_n) \in (\mathbb{Z}_q)^n$, and a functional decryption key $s_{\mathbf{y}}$ is related to a vector $\mathbf{y} = (y_1, \ldots, y_n) \in (\mathbb{Z}_q)^n$. Given a ciphertext and a secret key, the decryption algorithm computes the inner product $\langle \mathbf{y}, \mathbf{x} \rangle = \sum_{i=1}^{n} y_i x_i \in \mathbb{Z}_q$, that is,

$$F(\mathbf{y}, \mathbf{x}) = \sum_{i=1}^{n} y_i x_i \bmod q.$$

Notice that IPE is different from the inner-product predicate encryption presented in Subsection 6.3, where the ciphertext of a message m is related to a vector $\mathbf{x} \in (\mathbb{Z}_q)^n$, the secret key is related to a vector $\mathbf{y} \in (\mathbb{Z}_q)^n$, and the decryption algorithm reveals m if and only if $\langle \mathbf{x}, \mathbf{y} \rangle \equiv 0 \bmod q$. By contrast, the output in IPE schemes is the actual value of the inner product. At first glance, this functionality might seem less powerful than the previous definitions and constructions of identity-based encryption and attribute-based encryption. Indeed, inner product encryption cannot be used to construct those kinds of cryptosystems. However, neither IBE nor ABE can be used to build IPE. So this notion is completely separated from previous works, and its relevance stands in providing only partial information on the plaintext and not "all-or-nothing". Moreover, IPE directly finds many natural applications in theory as well as in practice. First, it can be used directly to compute the Hamming distance between two words, and more generally, the inner product is a distance for vectors of the fixed norm. So this could be exploited, for instance, in biometric identification. IPE could also be used in machine learning, where, for instance, Support Vector Machine evaluation can be just an inner product between a test vector and the data. In this case, a secret key could classify the data concerning one criterion and learn nothing about the rest of it. It also allows making statistical analysis, like weighted means or by encrypting the cross-products between the entries. It can even be used for computations of variance and other quadratic polynomials.

In [2], Abdalla et al. present a direct construction of public-key IPE relying on standard assumptions, such as LWE and DDH. The construction is only proved to be secure against selective adversaries who are asked to commit to their challenges at the beginning of the security game. In [16], Agrawal et al. provide constructions that provably achieve security against more realistic adaptive attacks, where the messages m_0 and m_1 may be adaptively chosen in the challenge phase. Later, in [15], Agrawal et al. prove that the scheme in [16] achieves adaptive SIM-based security (AD-SIM) rather than just adaptive IND-based security. Moreover, some IPE schemes based on the DDH, DCR, and LWE assumptions prove AD-SIM security for an unbounded number of key queries and a single challenge ciphertext.

In [30], Benhamouda et al. propose a generic construction for the first IND-CCA IPE schemes based on the DDH, DCR, and any of the MDDH assumptions. In [60], Castagnos et al. provide the first adaptive IND-secure IPE schemes, which allow for the evaluation of unbounded inner products modulo a prime p. The constructions rely on the assumption that supposes a DDH group containing a subgroup where the discrete logarithm problem is easy.

In [68], Chotard et al. present an IPE scheme for computing some weighted sums on aggregated encrypted data from standard assumptions in prime-order groups in the random oracle model.

Security of the mentioned IPE schemes is based on traditional number-theoretic assumptions, such as the hardness of factorisation and the discrete logarithm problem. However, the intractability of these number-theoretic problems will be extremely vulnerable due to Shor's algorithm [166] if the powerful quantum computers are built. In a recent work [158], Debnath et al. propose a multivariate cryptography-based inner-product encryption scheme. It is the first of its kind in the context of multivariate public-key cryptosystems. The authors use the technique of identity-based signature of [64] to develop this interesting scheme. The scheme attains non-adaptive SIM-based security under the hardness of the MQ problem.

7.1. FUNCTION-HIDING INNER PRODUCT ENCRYPTION. As reported in [32], in many real scenarios it is important to consider also the privacy of the computed function. Consider the following motivating example: suppose a hospital subscribes to a cloud service provider to store its patients' medical records. To protect the privacy of the data, these records are stored in an encrypted form. At a later point in time, the hospital can request the cloud to perform some analysis on the encrypted records by releasing a decryption key sk_f for a function f of its choice. If the FE scheme in use does not guarantee any hiding of the function (which is the case for many existing FE schemes), then the key sk_f might reveal f completely to the cloud, which is undesirable when f itself contains sensitive information. This has motivated the study of function privacy in FE, see for instance [164, 44, 55].

An IPE scheme is called *function-hiding* if the keys and ciphertexts reveal no additional information about the related vectors beyond their inner product. The *fully function-hiding* IPE achieves the most robust IND-based notion of both data and function privacy in the private-key setting in the standard model. We sketch here the model of full function privacy, as described in [7, 112]. Adversaries are allowed to interact with two *left-or-right* oracles $KeyGen_b(mk, \cdot, \cdot)$ and $Enc_b(mk, \cdot, \cdot)$ for a randomly chosen $b \in \{0, 1\}$, where $KeyGen_b$ takes two functions f_0 and f_1 as input and it returns a functional decryption key $sk_{f_b} = \texttt{KeyGen}(mk, f_b)$. The algorithm Enc_b takes two messages x_0 and x_1 as input and it outputs a ciphertext $c_{x_b} = \texttt{Enc}(mk, x_b)$. Adversaries can adaptively interact with oracles for any polynomial (a priori unbounded) number of queries. To exclude inherently inevitable attacks, there is a condition for adversarial queries that all pairs (x_0, x_1) and (f_0, f_1) must satisfy $f_0(x_0) = f_1(x_1)$.

Only two approaches have been proposed for (fully) function-private IPE schemes in the private-key setting. One is to employ the Brakerski-Segev general transformation from (non-function-private) FE schemes for general circuits [55]. The transformation itself is efficient since it simply combines symmetric key encryption with FE in a natural manner. Anyway, this approach requires computationally intensive cryptography tools, such as IND obfuscation[2], to realise non-function-private FE for general circuits, meaning it may be relatively inefficient overall. The other approach may be more practical. It directly constructs IPE schemes by using the dual-pairing vector spaces (DPVS) introduced by Okamoto and Takashima [140, 141].

In the last few years, there has been a flurry of works on the construction of function-hiding IPE, starting with the work of Bishop, Jain, and Kowalczyk [32]. They propose a function-hiding IPE scheme under the SXDH assumption, which

---

[2]In simple words, obfuscation aims to make a computer program "unintelligible" while preserving its functionality, and indistinguishability obfuscation requires that, given any two equivalent circuits of similar size, their obfuscation should be computationally indistinguishable.

satisfies an adaptive IND-based security definition. But the security model has one limitation: all ciphertext queries $\mathbf{x}_0, \mathbf{x}_1$ and all secret key queries $\mathbf{y}_0, \mathbf{y}_1$ are restrained by $\langle \mathbf{x}_0, \mathbf{y}_0 \rangle = \langle \mathbf{x}_0, \mathbf{y}_1 \rangle = \langle \mathbf{x}_1, \mathbf{y}_0 \rangle = \langle \mathbf{x}_1, \mathbf{y}_1 \rangle$. In [76], Datta et al. develop a full function-hiding IPE scheme built in the setting of asymmetric bilinear pairing groups of prime order. The security of the scheme is based on the well-studied SXDH assumption where the restriction on adversaries' queries is only $\langle \mathbf{x}_0, \mathbf{y}_0 \rangle = \langle \mathbf{x}_1, \mathbf{y}_1 \rangle$. Here, secret keys and ciphertexts of n-dimensional vectors consist of $4n + 8$ group elements. Tomida et al., in [173], construct a more efficient function-hiding IPE scheme than that of [76] under the XDLIN assumption, where secret keys and ciphertexts consist of $2n + 5$ group elements. Kim et al., in [111], put forth a fully-secure function-hiding IPE scheme with smaller parameter sizes and run-time complexity than those in [32, 76]. The scheme is proved SIM-based secure in the generic model of bilinear maps. In [187], Zhao et al. present the first SIM-based secure secret-key IPE scheme under the SXDH assumption in the standard model. The authors claim that the scheme can tolerate an unbounded number of ciphertext queries and adaptive key queries. Zhao et al. in [186] propose a new version of the scheme, which is an improvement in terms of computational and storage complexity. In a very recent work [125], Liu et al. present a more efficient and flexible private-key IPE scheme with SIM-based security. To ensure correctness, the scheme requires that the computation of inner products is within a polynomial range, where the discrete logarithm of $g^{\langle \mathbf{x}, \mathbf{y} \rangle}$ can be found in polynomial time. In [125, Table 2], the authors compare their proposed IPE scheme with those in [173, 76, 187, 186]. The performance of this scheme appears superior in both storage complexity and computation complexity. Moreover, secret keys and ciphertexts are shorter.

Although most aforementioned IPE schemes are efficient and based on standard assumptions, they all have one inconvenient property: they are *bounded*. The maximum length of vectors has to be fixed at the beginning, and afterward, one cannot handle vectors whose lengths exceed it. This could be inconvenient when it is hard to predict which data will be encrypted in the setup phase. One may think to solve the problem by setting the maximum length to a large value. However, the size of parameters expands at least linearly with the fixed maximum length, and such a solution incurs an unnecessary efficiency loss. In the context of IP-PE and ABE, there exist unbounded schemes (see, for instance, [56, 65, 118, 144]), whose public parameters do not impose a limit on the maximum length of vectors or number of attributes used in the scheme. In [174], Tomida and Takashima construct two concrete unbounded IPE schemes based on the standard SXDH assumption, both secure in the standard model: the first is a private-key IPE with fully function hiding, the second scheme is a public-key IPE with adaptive security. Concurrently and independently, in [82], Dufour-Sans and Pointcheval describe an unbounded IPE system supporting identity access control with succinct keys. Their construction is proved selectively IND-secure in the random oracle model based on the standard DBDH assumption. In [174, Table 1], it is shown a comparison, in terms of efficiency, among private-key schemes that are fully function hiding [75, 173, 112] and public-key schemes with adaptive security in the standard model [16].

7.2. Orthogonality FE. A variant of IPE is the so-called *Orthogonality FE* (OFE). In an OFE scheme, a ciphertext $c_\mathbf{x}$ is related to a vector $\mathbf{x} \in (\mathbb{Z}_q)^n$, and a functional decryption key $s_\mathbf{y}$ is related to a vector $\mathbf{y} \in (\mathbb{Z}_q)^n$. Given $c_\mathbf{x}$ and $s_\mathbf{y}$, the decryption algorithm determines if $\mathbf{x}$ is orthogonal to $\mathbf{y}$ or not. That is, it returns

1 if $\langle \mathbf{x}, \mathbf{y} \rangle = 0$, and returns 0 otherwise. At first glance, OFE appears as a simple modification of IPE, but the latter reveals more information on $\mathbf{x}$ and $\mathbf{y}$ than OFE does. Most of the existing OFE schemes are instantiated in (three-factors) composite-order bilinear groups [50, 110] or DPVS on prime-order bilinear groups [143, 145]. All of these schemes share a high level of conceptual complexity. In [180], Wee presents a family of simple OFE schemes in prime-order bilinear groups under the MDDH assumption. In [27], Barbosa et al. extend the Wee's work to the context of function-hiding.

8. OTHER FE SCHEMES

So far, we have mainly described schemes for predicate encryption and inner product encryption in their basic form. In this section, we want to mention other schemes: FE schemes that go beyond predicates and IPE and FE schemes beyond basic features.

8.1. FE FOR BOUNDED COLLUSIONS. When the security of an FE scheme is guaranteed only when a constant number of functional decryption keys are corrupted, we talk about *security for bounded collusions*. The case considered in general is the *unbounded collusions* one. Sahai and Seyalioglu [159] build the first FE scheme for all circuits where security handles the corruption of one functional decryption key. The scheme uses garbles circuits and public-key encryption, and the ciphertext size depends on the size of the circuit associated with the functional decryption keys. Improvements are presented in [98] in which the ciphertext size depends only on the size of the output of the function for which the functional decryption keys are generated. This scheme uses ABE for all circuits and FHE, both admitting constructions from standard assumptions. The works in [99, 8] show how to generically turn any FE scheme secure only when one functional decryption key is corrupted into an FE scheme where security handles an (a priori bounded) polynomial number of collusions.

8.2. FE SCHEMES FOR QUADRATIC FUNCTIONS. With the FE scheme for quadratic functions, we intend to allow bilinear maps computing over the integers. In particular, messages are expressed as pairs of vectors $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}^n \times \mathbb{Z}^m$ and secret keys are associated with matrices $\mathbf{A} = (a_{ij}) \in \mathbb{Z}^{n \times m}$. The decryption allows to compute

$$\mathbf{x}^\top \mathbf{A} \mathbf{y} = \sum_{i,j} a_{ij} x_i y_j.$$

Bilinear maps have several practical applications: for instance, a quadratic polynomial can express different statistical functions (e.g., mean, variance, covariance), the Euclidean distance between two vectors, and the application of a linear or quadratic classifier. FE for an inner product can be used as the building block to obtain FE for quadratic functions. This fact, implicit in [26], is made explicit in [91] and in the private-key variants [123, 22]. All the schemes in the works mentioned above have been constructed from standard assumptions on pairings.

In particular, in [26] Baltico et al. present two efficient FE schemes for quadratic functions with linear-size ciphertexts in the public-key setting. One scheme is proved selective IND-secure under standard assumptions (MDDH and 3PDDH), the other is proved adaptive IND-secure in the generic-group model. Moreover, in [26, Table 1], its comparison is presented with different schemes for quadratic functions (some of which are in the private-key setting). Further results have been obtained in

[181], where Wee presents a scheme with constant-size keys and short ciphertexts (selective SIM-based secure on standard assumptions).

8.3. FE schemes for circuits. We now consider functionalities of a more general form: arbitrary circuits. Some results have been obtained for PE schemes for circuits. In [101], Gorbunov et al. present a leveled PE scheme for all circuits (Boolean predicates of bounded depth), with succinct ciphertexts and secret keys independent of the size of the circuit. The achieved privacy notion is a selective SIM-based variant of attribute-hiding, assuming the hardness of the subexponential LWE problem. Recall that the strong variant notion (full attribute-hiding) is impossible to realise for many messages [47, 12].

Some results have also been obtained for general-purpose FE, in which functions associated with secret keys can be any arbitrary circuits. In Subsection 8.1 some results for bounded collusions are presented. In [88], Garg et al. give constructions for IND obfuscation (based on multilinear maps), and they use it to construct FE for all polynomial-size circuits. In [43, 89], there are constructions directly based on multilinear maps. Further analysis can be found in [124] where Lin and Tessaro reduce the degree of the required multilinear map to 3.

8.4. Multi-input FE. *Multi-Input Functional Encryption* (MI-FE) is a generalisation of functional encryption to the setting of multi-input functions. The functions, evaluated on encrypted information, can be assumed to take multiple inputs, and each input corresponding to a different ciphertext. That is, the scheme has several encryption slots and each secret key sk_f for a multi-input function f decrypts jointly ciphertexts $\mathtt{Enc}(x_1), \ldots, \mathtt{Enc}(x_n)$ for all slots to obtain $f(x_1, \ldots, x_n)$ without revealing anything more about the encrypted messages. The MI-FE functionality provides the capability to independently encrypt messages for different slots. This concept was introduced by Goldwasser et al. in [97].

Abdalla et al. in [6] construct the first scheme of Multi-Input Inner Product Encryption (MI-IPE) which achieves message privacy, and Datta et al., in [77], propose a new scheme which they call *unbounded private-key* MI-IPE. It achieves function-hiding privacy; meanwhile, they enable the encryption of ciphertexts and the generation of secret keys for unbounded vectors. While the inner product functionality is helpful for several meaningful applications (we refer the reader to [6] for a discussion), it is evidently desirable, from the viewpoint of both theory and practice, to extend the reach of MI-FE from standard assumptions beyond inner products. In [4], Abdalla et al. put forward a novel methodology to convert single-input FE for inner products into multi-input schemes for the same functionality. The resulting scheme does not require pairings, it can be instantiated with all known single-input schemes and it relies on different assumptions, such as DDH, LWE, and DCR. In a very recent preprint, [13], Agrawal et al. present the first MI-FE scheme for quadratic functions from pairings. All previous MI-FE schemes either support only inner products (linear functions) or rely on solid cryptographic assumptions such as indistinguishability obfuscation or multilinear maps. The scheme showed in [13] would achieve (selective) IND-based security against unbounded collusions under the standard BMDDH assumption. Thus, their construction would accomplish the same level of protection as single input quadratic FE.

In [10], the notion of *Ad Hoc MI-FE* (aMI-FE) was introduced to handle the key escrow problem of MI-FE. aMI-FE does not differentiate between key authorities and users, and it lets users generate their own partial decryption keys along with

ciphertexts. In the same work, Agrawal et al. provide construction of aMI-FE for inner product based on the LWE assumption.

Recently, Agrawal, Goyal, and Tomida in [14] define *Multi-Party Functional Encryption* (MP-FE), which extends and abstracts various notions of functional encryption such as multi-input, multi-client, multi-authority, and dynamic decentralised that we present in the following sections. MP-FE allows for distributed ciphertexts and distributed keys and specifies how these may be combined for function evaluation. It comprehends both key-policy and ciphertext-policy schemes, and it captures both attribute and function hiding. It also supports schemes with interactive, independent, or centralised setup. The authors individuate several combinations of features not studied in literature and provide constructions for some of them with their general framework.

8.5. MULTI-CLIENT FE. *Multi-Client Functional Encryption* (MC-FE), as defined in [97], generalises the definition of functional encryption in the following way. The single input $x \in X$ to the encryption procedure is divided into n independent components $(x_1, \ldots, x_n)$. Each client C_i does the following encryption $\texttt{Enc}(\text{pk}, \text{ek}_i, x_i, \ell)$, where ℓ is a label, usually time-dependent, and ek_i is an encryption key specific for the client C_i. A user owning a secret key sk_f for an n-ary function f and n ciphertexts $\texttt{Enc}(\text{pk}, \text{ek}_1, x_1, \ell)$, ..., $\texttt{Enc}(\text{pk}, \text{ek}_n, x_n, \ell)$ can compute $f(x_1, \ldots, x_n)$ but he will learn nothing else about each x_i. The difference with Multi-Input FE is that the combination of ciphertexts generated for different labels (hence at other times) does not give a valid global ciphertext, and the adversary learns nothing from it. In MI-FE, every ciphertext from every slot can be combined with any other ciphertext from any different slot. The first MC-FE for an inner product in the standard model (under LWE assumption) can be found in [121]. Other MC-FE schemes can be found in [70, 3].

8.6. MULTI-AUTHORITY AND DECENTRALISED FE. A drawback of standard FE is that a single party, the authority, is responsible for creating the functional decryption keys for all users in the system. As a direct consequence, this authority can decrypt all messages since the authority has to create every possible decryption key. Thus, relying on a single authority has consequences for the scalability of the system and the trust relations. In practical situations, we would instead appoint multiple authorities, where each authority is responsible for issuing keys but cannot decrypt messages unless it cooperates with (all) other authorities. The question of whether it is possible to construct such a *multi-authority scheme* was first raised by Sahai and Waters [160]. Whereas in [117], Lewko and Waters address both trust and scalability issues rather: no authority is required to hold a master key, and new authorities can be added to the system without requiring any form of interaction. The resulting scheme is so-called a *decentralised* FE scheme.

8.6.1. **Multi-authority FE.** In a *Multi-Authority Predicate Encryption* (MA-PE) system, ciphertexts are associated with one or more predicates from various authorities. Only users with keys satisfying all these predicates can decrypt the ciphertext. The first proposed MA-PE schemes either require interaction between all authorities [61, 136], or do not allow for the addition of new authorities once the system is set up [62]. They are all multi-authority attribute-based encryption (MA-ABE), and they are based on the DBDH assumption. Further results on MA-ABE scheme can be found in [129, 130, 119]. The *Controlled Functional Encryption* (C-FE), introduced by Naveed et al. [138], is a special flavor of FE. In C-FE, the decryption

algorithm becomes a two-party protocol between the party holding the function key and the authority, where only the former learns the output of the computation. In a very recent work [19], Ambrona et al. extend C-FE to a multi-authority C-FE by distributing the role of (and the trust in) the authority across several parties.

8.6.2. **Decentralised FE.** As above-mentioned, the first FE scheme that does not require a trusted authority is due to Lewko and Waters, [117]. It is a decentralised MA-ABE, where each authority works completely separately, and failures or disruptions for some authorities will not affect other authorities. This makes the system stronger than the majority of MA-ABE schemes. Apart from the initial set of public parameters built by all authorities, authorities no longer need to establish trustable relationships with each other in advance. Other decentralised MA-ABE can be found in [122, 62, 156, 183]. In all these works, collusion resistance is obtained using a *Global Identifier* (GID), but this can breach the user privacy. In [183], this issue is studied: unique user identifiers are obtained by combining a user's identity with the identity of the (local) attribute authority (AA) where the user is located. The user identities remain private to the AA outside the domain, which enhances privacy and security. The scheme is based on composite-order bilinear groups and some variants of SD3, whereas security proof makes use of the dual system encryption methodology (for more details, see [178] where this methodology is first introduced).

In [175], van de Kamp et al. propose a generic framework for creating decentralised multi-authority predicate encryption. The framework supports several predicate types, such as MA-IBE, MA-ABE, and MA-IP-PE. In the random oracle model, the resulting encryption schemes are proved fully secure under standard subgroup decision assumptions, formulated for a bilinear group of orders a product of 3 primes.

The definition of MC-FE stated in Subsection 8.5 assumes the existence of a trusted third party who runs the `Setup` algorithm and distributes the functional decryption keys. As introduced in [69], in a Decentralised MC-FE (DMC-FE), the authority is removed, and the clients work together to generate appropriate functional decryption keys. In [69], Chotard et al. give the first DMC-FE from standard assumptions for inner products. Security is proved using bilinear pairing groups, and the scheme handles the corruption of input slots. In [121], Libert and Ţiţiu present the first decentralised MC-FE scheme based on LWE assumptions. In [1], Abdalla et al. provide a generic compiler from any MC-FE scheme satisfying an extra property, called *special key derivation*[3], into a DMC-FE scheme. The transformation is purely information-theoretic, and it does not require any additional assumptions. As the MC-FE from Chotard et al. [69] satisfies this extra property, the resulting scheme is a DMC-FE scheme secure under the basic DDH assumption without pairings (in the random oracle model). As in [69], the version of the scheme without labels is secure in the standard model.

In [68], Chotard et al. introduce the *Dynamic Decentralised Functional Encryption* (DD-FE), a generalisation of FE which allows multiple users to join the system

---

[3]In a MI-FE or MC-FE scheme with the *special key derivation* property the master secret key can be split into separate secret keys, one for each input, i.e. $mk = \{mk_i\}_{i=1,...,n}$, and functional decryption keys sk_f are derived through a combination of local and linear inner-product computations on i, f, sk_i and pp.

dynamically, without relying on a trusted third party or expensive and interactive Multi-Party Computation protocols. This notion subsumes existing multi-user extensions of FE, such as Multi-Input, Multi-Client, and Multi-Party FE.

8.7. HIERARCHICAL FE. Motivated by the applicability of functional encryption to expressive access control systems, the *Hierarchical Functional Encryption* has been introduced by Ananth et al. in [20]. In a hierarchical FE scheme, the holder of any functional decryption key sk_f for a function f can in turn generate a functional decryption key $sk_{g \circ f}$ corresponding to the function $g \circ f$ for any given function g. Now, anyone holding the delegated functional key $sk_{g \circ f}$ and an encryption of any message x can compute $g(f(x))$, but cannot learn any additional information about the message x and $f(x)$. Such expressive delegation capabilities give rise to hierarchical access-control, a sought-after ingredient in modern access control systems. In particular, the notion of hierarchical FE generalises those of HIBE and HABE (see Paragraph 5.1.1 and Paragraph 5.2.5). In [54], Brakerski et al. present a generic transformation that converts any general-purpose public-key FE scheme into a hierarchical one without relying on any additional assumptions. This construction yields various hierarchical schemes based on various assumptions in the standard model, such as multilinear maps and the LWE assumption.

8.8. TRACEABLE FE. The conventional definition of FE associates each function to a secret functional decryption key, and therefore, all users get the same private key for the same function. This induces an important problem: if one of these users (called a *traitor*) leaks or sells a functional decryption key to be included in a pirate decryption tool, then there is no way to trace back its identity. *Traitor tracing* is a mechanism enabling an authority or an arbitrary party (a delegated party in the system with this specific task) to identify malicious users who possibly colluded. Several IBE [5, 102, 24, 154] and ABE [139, 126, 127, 128] schemes take into consideration the traceability. Indeed, achieving traceability is usually very expensive. Adding traitor tracing to public-key encryption requires a very high extra cost: even in the bounded model, the cost grows proportionally with the number of traitors. In [81], a new primitive, called *Traceable Functional Encryption*, is defined. The functional decryption key will not only be specific to a function but to a user too, in such a way that if some users collude to produce a pirate decoder that successfully evaluates a function on the plaintext, from the ciphertext only, one can trace back at least one of them. In [81], Do et al. propose a traceable IP-FE with black-box confirmation, using the pairing.

8.9. VERIFIABLE FE. In the standard setting of FE, authority and the encryptors are supposed to run their respective algorithms faithfully. In [171], Tang and Ji introduce the notion of *verifiable ABE* (VABE), where it is checked whether the functional decryption keys have been generated correctly. The core idea of the method is using some trick to change secret sharing [162] in the ABE schemes with verifiable secret sharing [170]. In [25], Badrinarayanan et al. extend the VABE to the concept of *verifiable FE* (VFE), which essentially guarantees that dishonest encryptors and authorities, even when colluding together, are not able to generate ciphertexts and functional decryption keys that give "inconsistent" results. But, the solution proposed in [25] is not applicable for the IPE scheme since it requires a perfectly correct IPE scheme. For this reason, in [168], Soroush et al. improve (in terms of efficiency) the construction in [25] and they construct the first efficient perfectly correct IPE scheme, whose security relies on the DLIN assumption.

9. Conclusions

In this paper, we summarise the state-of-the-art for Functional Encryption schemes. We provide an overview of the main mathematical assumptions used for proving the security of FE schemes and explicitly exhibit some connections between these assumptions. We also give an overview of the used security models. For IBE, ABE, Predicate Encryption with private index, and Inner Product Encryption, we describe the basic structure of the schemes and present their main characteristics. For each class of FE schemes, we provide several references to the reader, focusing on the works that first offered a practical construction and the most recent constructions. Finally, we present schemes that go beyond the inner product and schemes with enhanced features. The latter comprehend schemes useful in real-life scenarios.

In this survey, we give great relevance to the mathematical assumptions which many FE schemes rely upon. We observe that there are assumptions not quantum-resistant or hardly realisable at the basis of many constructions. The latter means that there are few explicit examples of algebraic structures which satisfy the given assumption. For this reason, in our opinion, more work should be done to obtain solutions which are safer and more practical.

Even though FE schemes can be helpful for different applications and different real scenarios, as described in Section 7 and 8, to our knowledge, the only practical implementations of FE schemes belong to the class of IBE and ABE. These classes are undoubtedly the most studied because they are chronologically the first to appear and because many works focus on efficient constructions of these schemes. For the other classes, to our knowledge, we can only find some theoretical analyses of the systems, but actual implementations are still missing. Indeed, in scenarios where there is the need to learn a function of the encrypted data, FHE or similar schemes are so far preferred.

Nevertheless, since FE schemes have great potential, we believe that their research will still be flourishing in the following years.

Acknowledgments

References

[1] M. Abdalla, F. Benhamouda, M. Kohlweiss and H. Waldner, Decentralizing inner-product functional encryption, In *IACR International Workshop on Public Key Cryptography*, **11443** (2019), 128–157.

[2] M. Abdalla, F. Bourse, A. D. Caro and D. Pointcheval, Simple functional encryption schemes for inner products, In *IACR International Workshop on Public Key Cryptography*, **9020** (2015), 733–751.

[3] M. Abdalla, F. Bourse, H. Marival, D. Pointcheval, A. Soleimanian and H. Waldner, Multi-client inner-product functional encryption in the random-oracle model, In *International Conference on Security and Cryptography for Networks*, **12238** (2020), 525–545.

[4] M. Abdalla, D. Catalano, D. Fiore, R. Gay and B. Ursu, Multi-input functional encryption for inner products: Function-hiding realizations and constructions without pairings, In *Annual International Cryptology Conference*, **10991** (2018), 597–627.

[5] M. Abdalla, A. W. Dent, J. Malone-Lee, G. Neven, D. Hieu Phan and N. P Smart, Identity-based traitor tracing, In *International Workshop on Public Key Cryptography*, **4450** (2007), 361–376.

[6] M. Abdalla, R. Gay, M. Raykova and H. Wee, Multi-input inner-product functional encryption from pairings, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **10210** (2017), 601–626.

[7] S. Agrawal, S. Agrawal, S. Badrinarayanan, A. Kumarasubramanian, M. Prabhakaran and A. Sahai, On the practical security of inner product functional encryption, In *IACR International Workshop on Public Key Cryptography*, **9020** (2015), 777–798.

[8] S. Agrawal, Stronger security for reusable garbled circuits, general definitions and attacks, In *Annual International Cryptology Conference*,**10401** (2017), 3–35.

[9] S. Agrawal, D. Boneh and X. Boyen, Efficient lattice (H) IBE in the standard model, In*Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **6110** (2010), 553–572.

[10] S. Agrawal, M. Clear, O. Frieder, S. Garg, A. O'Neill and J. Thaler, Ad hoc multi-input functional encryption, In *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*, Leibniz International Proceedings in Informatics (LIPIcs), Schloss Dagstuhl-Leibniz-Zentrum für Informatik, **151** (2020), 1–41.

[11] S. Agrawal, D. M. Freeman and V. Vaikuntanathan, Functional encryption for inner product predicates from learning with errors, In *International Conference on the Theory and Application of Cryptology and Information Security*, **7073** (2011), 21–40.

[12] S. Agrawal, S. Gorbunov, V. Vaikuntanathan and H. Wee, Functional encryption: New perspectives and lower bounds, In *Annual Cryptology Conference*, **8043** (2013), 500–518.

[13] S. Agrawal, R. Goyal and J. Tomida, *Multi-Input Quadratic Functional Encryption From Pairings*, Cryptology ePrint Archive, Report 2020/1285, 2020, https://eprint.iacr.org/2020/1285.

[14] S. Agrawal, R. Goyal and J. Tomida, *Multi-Party Functional Encryption*, Cryptology ePrint Archive, Report 2020/1266, 2020, https://eprint.iacr.org/2020/1266.

[15] S. Agrawal, B. Libert, M. Maitra and R. Titiu, Adaptive simulation security for inner product functional encryption, In *IACR International Conference on Public-Key Cryptography*, Springer, Cham, **12110** (2020), 34–64.

[16] S. Agrawal, B. Libert and D. Stehlé, Fully secure functional encryption for inner products, from standard assumptions, In *Annual International Cryptology Conference*, **9816** (2016), 333–362.

[17] R. R. Al-Dahhan, Q. Shi, G. Myoung Lee and K. Kifayat, Survey on revocation in ciphertext-policy attribute-based encryption, *Sensors*, **19** (2019).

[18] J. Alwen, M. Barbosa, P. Farshim, R. Gennaro, S. Gordon, S. Tessaro and D. A. Wilson, On the relationship between functional encryption, obfuscation, and fully homomorphic encryption, In *IMA International Conference on Cryptography and Coding*, **8308** (2013), 65–84.

[19] M. Ambrona, D. Fiore and C. Soriente, Controlled functional encryption revisited: Multi-authority extensions and efficient schemes for quadratic functions, *Proceedings on Privacy Enhancing Technologies*, **2021** (2021), 21–42.

[20] P. Ananth, D. Boneh, S. Garg, A. Sahai and M. Zhandry, *Differing-Inputs Obfuscation and Applications*, Cryptology ePrint Archive, Report 2013/689, 2013, https://eprint.iacr.org/2013/689.

[21] P. Ananth, Z. Brakerski, G. Segev and V. Vaikuntanathan, From Selective to Adaptive Security in Functional Encryption, In *Annual Cryptology Conference*, **9216** (2015), 657–677.

[22] P. Ananth and A. Sahai, Projective arithmetic functional encryption and indistinguishability obfuscation from degree-5 multilinear maps, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **10210** (2017), 152–181.

[23] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. De Panafieu and C. Ràfols, Attribute-based encryption schemes with constant-size ciphertexts, *Theoret. Comput. Sci.*, **422** (2012), 15–38.

[24] M. Au, Q. Huang, J. K. Liu, W. Susilo, D. S. Wong and G. Yang, Traceable and retrievable identity-based encryption, In *International Conference on Applied Cryptography and Network Security*, **5037** (2008), 94–110.

[25] S. Badrinarayanan, V. Goyal, A. Jain and A. Sahai, Verifiable functional encryption, In *International Conference on the Theory and Application of Cryptology and Information Security*, **10032** (2016), 557–587.

[26] C. E. Z. Baltico, D. Catalano, D. Fiore and R. Gay, Practical functional encryption for quadratic functions with applications to predicate encryption, In *Annual International Cryptology Conference*, **10401** (2017), 67–98.

[27] M. Barbosa, D. Catalano, A. Soleimanian and B. Warinschi, Efficient function-hiding functional encryption: From inner-products to orthogonality, In *Cryptographers' Track at the RSA Conference*, **11405** (2019), 127–148.

[28] J. Bartusek, B. Carmer, A. Jain, Z. Jin, T. Lepoint, F. Ma, T. Malkin, A. J. Malozemoff and M. Raykova, Public-key function-private hidden vector encryption (and more), In *International Conference on the Theory and Application of Cryptology and Information Security*, **11923** (2019), 489–519.

[29] M. Bellare and P. Rogaway, Random oracles are practical: A paradigm for designing efficient protocols, In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, (1993), 62–73.

[30] F. Benhamouda, F. Bourse and H. Lipmaa, CCA-secure inner-product functional encryption from projective hash functions, In *IACR International Workshop on Public Key Cryptography*, **10175** (2017), 36–66.

[31] J. Bethencourt, A. Sahai and B. Waters, Ciphertext-policy attribute-based encryption, In *2007 IEEE Symposium on Security and Privacy (SP'07)*, (2007), 321–334.

[32] A. Bishop, A. Jain and L. Kowalczyk, Function-hiding inner product encryption, In *International Conference on the Theory and Application of Cryptology and Information Security*, **9452** (2015), 470–491.

[33] I. F. Blake, V. K. Murty and G. Xu, Refinements of Miller's algorithm for computing the Weil/Tate pairing, *J. Algorithms*, **58** (2006), 134–149.

[34] O. Blazy, L. Brouilhet and D. H. Phan, Anonymous identity based encryption with traceable identities, In *Proceedings of the 14th International Conference on Availability, Reliability and Security*, (2019), 1–10.

[35] D. Boneh and X. Boyen, Efficient selective-ID secure identity-based encryption without random oracles, In *International Conference on the Theory and Applications of Cryptographic Techniques*, **3027** (2004), 223–238.

[36] D. Boneh and X. Boyen, Secure identity based encryption without random oracles, In *Annual International Cryptology Conference*, **3152** (2004), 443–459.

[37] D. Boneh, X. Boyen and E.-J. Goh, Hierarchical identity based encryption with constant size ciphertext, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **3494** (2005), 440–456.

[38] D. Boneh, X. Boyen and H. Shacham, Short group signatures, In *Annual International Cryptology Conference*, **3152** (2004), 41–55.

[39] D. Boneh, G. D. Crescenzo, R. Ostrovsky and G. Persiano, Public key encryption with keyword search, In *International Conference on the Theory and Applications of Cryptographic Techniques*, **3027** (2004), 506–522.

[40] D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, In *Annual International Cryptology Conference*, **2139** (2001), 213–229.

[41] D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan and D. Vinayagamurthy, Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **8441** (2014), 533–556.

[42] D. Boneh, C. Gentry and M. Hamburg, Space-efficient identity based encryptionwithout pairings, In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*, (2007), 647–657.

[43] D. Boneh, K. Lewi, M. Raykova, A. Sahai, M. Zhandry and J. Zimmerman, Semantically secure order-revealing encryption: Multi-input functional encryption without obfuscation, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **9057** (2015), 563–594.

[44] D. Boneh, A. Raghunathan and G. Segev, Function-private identity-based encryption: Hiding the function in functional encryption, In *Annual Cryptology Conference*, **8043** (2013), 461–478.

[45] D. Boneh, A. Raghunathan and G. Segev, Function-private subspace-membership encryption and its applications, In *International Conference on the Theory and Application of Cryptology and Information Security*, **8269** (2013), 255–275.

[46] D. Boneh, A. Sahai and B. Waters, Fully collusion resistant traitor tracing with short ciphertexts and private keys, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **4004** (2006), 573–592.

[47] D. Boneh, A. Sahai and B. Waters, Functional encryption: Definitions and challenges, In *Theory of Cryptography Conference*, **6597** (2011), 253–273.

[48] D. Boneh, A. Sahai and B. Waters, Functional encryption: A new vision for public-key cryptography, *Communications of the ACM*, **55** (2012), 56–64.

[49] D. Boneh and A. Silverberg, Applications of multilinear forms to cryptography, *Contemp. Math.*, **324** (2003), 71–90.

[50] D. Boneh and B. Waters, Conjunctive, subset, and range queries on encrypted data, In *Theory of Cryptography Conference*, **4392** (2007), 535–554.

[51] X. Boyen, Multipurpose identity-based signcryption: A Swiss Army knife for identity-based cryptography, In *Annual International Cryptology Conference*, **2729** (2003), 383–399.

[52] X. Boyen, A tapestry of identity-based encryption: Practical frameworks compared, *Int. J. Appl. Cryptogr.*, **1** (2008), 3–21.

[53] X. Boyen and B. Waters, Anonymous hierarchical identity-based encryption (without random oracles), In *Annual International Cryptology Conference*, **4117** (2006), 290–307.

[54] Z. Brakerski, N. Chandran, V. Goyal, A. Jain, A. Sahai and G. Segev, Hierarchical functional encryption, In *8th Innovations in Theoretical Computer Science Conference (ITCS 2017)*, *Leibniz Int. Proc. Inform. (LIPIcs)*, **67** (2017), 1–27.

[55] Z. Brakerski and G. Segev, Function-private functional encryption in the private-key setting, *J. Cryptology*, **31** (2018), 202–225.

[56] Z. Brakerski and V. Vaikuntanathan, Circuit-ABE from LWE: Unbounded attributes and semi-adaptive security, In *Annual International Cryptology Conference*, **9816** (2016), 363–384.

[57] J. Camenisch, M. Kohlweiss, A. Rial and C. Sheedy, Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data, In *International Workshop on Public Key Cryptography*, **5443** (2009), 196–214.

[58] R. Canetti, S. Halevi and J. Katz, A forward-secure public-key encryption scheme, In *International Conference on the Theory and Applications of Cryptographic Techniques*, **2656** (2003), 255–271.

[59] D. Cash, D. Hofheinz, E. Kiltz and C. Peikert, Bonsai trees, or how to delegate a lattice basis, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **6110** (2010), 523–552.

[60] G. Castagnos, F. Laguillaumie and I. Tucker, Practical fully secure unrestricted inner product functional encryption modulo p, In *International Conference on the Theory and Application of Cryptology and Information Security*, **11273** (2018), 733–764.

[61] M. Chase, Multi-authority attribute based encryption, In *Theory of Cryptography Conference*, **4392** (2007), 515–534.

[62] M. Chase and S. S. Chow, Improving privacy and security in multi-authority attribute-based encryption, In *Proceedings of the 16th ACM Conference on Computer and Communications Security*, (2009), 121–130.

[63] S. Chatterjee and P. Sarkar, Trading time for space: Towards an efficient IBE scheme with short(er) public parameters in the standard model, In *International Conference on Information Security and Cryptology*, **3935** (2005), 424–440.

[64] J. Chen, J. Ling, J. Ning and J. Ding, Identity-based signature schemes for multivariate public key cryptosystems, *Comput. J.*, **62** (2019), 1132–1147.

[65] J. Chen, J. Gong, L. Kowalczyk and H. Wee, Unbounded ABE via bilinear entropy expansion, revisited, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **10820** (2018), 503–534.

[66] J. Chen and H. Wee, Fully,(almost) tightly secure IBE and dual system groups, In *Annual Cryptology Conference*, **8043** (2013), 435–460.

[67] J. H. Cheon, K. Han, C. Lee, H. Ryu and D. Stehlé, Cryptanalysis of the multilinear map over the integers, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **9056** (2015), 3–12.

[68] J. Chotard, E. Dufour-Sans, R. Gay, D. H. Phan and D. Pointcheval, Dynamic decentralized functional encryption, In *Annual International Cryptology Conference*, **12170** (2020) 747–775.

[69] J. Chotard, E. D. Sans, R. Gay, D. H. Phan and D. Pointcheval, Decentralized multi-client functional encryption for inner product, In *International Conference on the Theory and Application of Cryptology and Information Security*, **11273** (2018), 703–732.

[70] M. Ciampi, L. Siniscalchi and H. Waldner, Multi-client functional encryption for separable functions, In *Public-Key Cryptography - PKC 2021 - 24th IACR International Conference on Practice and Theory of Public Key Cryptography, Virtual Event, May 10-13, 2021, Proceedings, Part I*, volume 12710 of *Lecture Notes in Computer Science*, pages 724–753. Springer, 2021.

[71] C. Cocks, An identity based encryption scheme based on quadratic residues, In *IMA International Conference on Cryptography and Coding*, **2260** (2001), 360–363.

[72] J.-S. Coron, T. Lepoint and M. Tibouchi, Practical multilinear maps over the integers, In *Annual Cryptology Conference*, **8042** (2013), 476–493.

[73] H. Cui, T. H. Yuen, R. H. Deng and G. Wang, Server-aided revocable attribute-based encryption for cloud computing services, *Concurrency and Computation: Practice and Experience*, **32** (2020).

[74] R. M. Daniel, E. B. Rajsingh and S. Silas, Analysis of hierarchical identity based encryption schemes and its applicability to computing environments, *J. Information Security and Applications*, **36** (2017), 20–31.

[75] P. Datta, R. Dutta and S. Mukhopadhyay, Functional encryption for inner product with full function privacy, In *Public-Key Cryptography–PKC 2016*, **9614** (2016), 164–195.

[76] P. Datta, R. Dutta and S. Mukhopadhyay, Strongly full-hiding inner product encryption, *Theoret. Comput. Sci.*, **667** (2017), 16–50.

[77] P. Datta, T. Okamoto and J. Tomida, Full-hiding (unbounded) multi-input inner product functional encryption from the k-linear assumption, In *IACR International Workshop on Public Key Cryptography*, **10770** (2018), 245–277.

[78] A. D. Caro, V. Iovino and G. Persiano, Fully secure hidden vector encryption, In *International Conference on Pairing-Based Cryptography*, **7708** (2012), 102–121.

[79] De Componendis Cifris, Functional Encryption, an overview - Carla Mascia, Irene Villa, https://www.youtube.com/watch?v=jz8v22jDlAs, https://www.decifris.it/cifrisCloud. Accessed: 2021-08-12.

[80] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu and W. Shi, Ciphertext-policy hierarchical attribute-based encryption with short ciphertexts, *Inform. Sci.*, **275** (2014), 370–384.

[81] X. T. Do, D. H. Phan and D. Pointcheval, Traceable inner product functional encryption, In *Cryptographers' Track at the RSA Conference*, **12006** (2020), 564–585.

[82] E. Dufour-Sans and D. Pointcheval, Unbounded inner-product functional encryption with succinct keys, In *International Conference on Applied Cryptography and Network Security*, **11464** (2019), 426–441.

[83] A. Escala, G. Herold, E. Kiltz, C. Rafols and J. Villar, An algebraic framework for Diffie–Hellman assumptions, *J. Cryptology*, **30** (2017), 242–288.

[84] C.-I. Fan and Y.-F. Tseng, Anonymous multi-receiver identity-based authenticated encryption with CCA security, *Symmetry*, **7** (2015), 1856–1881.

[85] M. Fischlin, A. Lehmann, T. Ristenpart, T. Shrimpton, M. Stam and S. Tessaro, Random oracles with (out) programmability, In *International Conference on the Theory and Application of Cryptology and Information Security*, **6477** (2010), 303–320.

[86] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, A Series of Books in the Mathematical Sciences. W. H. Freeman and Co., San Francisco, Calif., 1979.

[87] S. Garg, C. Gentry and S. Halevi, Candidate multilinear maps from ideal lattices, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **7881** (2013), 1–17.

[88] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai and B. Waters, Candidate indistinguishability obfuscation and functional encryption for all circuits, *SIAM J. Comput.*, **45** (2016), 882–929.

[89] S. Garg, C. Gentry, S. Halevi and M. Zhandry, Functional encryption without obfuscation, In *Theory of Cryptography Conference*, **9563** (2016), 480–511.

[90] R. Gay, *Public-Key Encryption, Revisited: Tight Security and Richer Functionalities*, PhD thesis, PSL Research University, 2019.

[91] R. Gay, A new paradigm for public-key functional encryption for degree-2 polynomials, In *IACR International Conference on Public-Key Cryptography*, **12110** (2020), 95–120.

[92] C. Gentry, Practical identity-based encryption without random oracles, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **4004** (2006), 445–464.

[93] C. Gentry, Fully homomorphic encryption using ideal lattices, *STOC'09¡¼Proceedings of the 2009 ACM International Symposium on Theory of Computing, ACM, New York*, (2009), 169–178.

[94] C. Gentry, S. Gorbunov and S. Halevi, Graph-induced multilinear maps from lattices, In *Theory of Cryptography Conference*, **9015** (2015), 498–527.

[95] C. Gentry and A. Silverberg, Hierarchical ID-based cryptography, In *International Conference on the Theory and Application of Cryptology and Information Security*, **2501** (2002), 548–566.

[96] F. Giacon, R. Aragona and M. Sala, A proof of security for a key-policy RS-ABE scheme, *JP J. Algebra, Number Theory and Applications*, **40** (2018), 29–90.

[97] S. Goldwasser, S. D. Gordon, V. Goyal, A. Jain, J. Katz, F.-H. Liu, A. Sahai, E. Shi and H.-S. Zhou, Multi-input functional encryption, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **8441** (2014), 578–602.

[98] S. Goldwasser, Y. Kalai, R. A. Popa, V. Vaikuntanathan and N. Zeldovich, Reusable garbled circuits and succinct functional encryption, In*Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, (2013), 555–564.

[99] S. Gorbunov, V. Vaikuntanathan and H. Wee, Functional encryption with bounded collusions via multi-party computation, In *Annual Cryptology Conference*, **7417** (2012), 162–179.

[100] S. Gorbunov, V. Vaikuntanathan and H. Wee, Attribute-based encryption for circuits, *J. ACM (JACM)*, **62** (2015), 1–33.

[101] S. Gorbunov, V. Vaikuntanathan and H. Wee, Predicate encryption for circuits from LWE, In *Annual Cryptology Conference*, **9216** (2015), 503–523.

[102] V. Goyal, Reducing trust in the PKG in identity based cryptosystems, In *Annual International Cryptology Conference*, **4622** (2007), 430–447.

[103] V. Goyal, O. Pandey A. Sahai and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, In *Proceedings of the 13th ACM Conference on Computer and Communications Security*, (2006), 89–98.

[104] G. Hanaoka, M. Komatsu, K. Ohara, Y. Sakai and S. Yamada, Semantic definition of anonymity in identity-based encryption and its relation to indistinguishability-based definition, In *European Symposium on Research in Computer Security*, (2020), 65–85.

[105] G. Hanaoka and S. Yamada, A survey on identity-based encryption from lattices, In *Mathematical Modelling for Next-Generation Cryptography*, **29** (2018), 349–365.

[106] K. He, J. Weng, J.-N. Liu, J. K. Liu, W. Liu and R. H. Deng, Anonymous identity-based broadcast encryption with chosen-ciphertext security, In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, (2016), 247–255.

[107] J. Horwitz and B. Lynn, Toward hierarchical identity-based encryption, In *International Conference on the Theory and Applications of Cryptographic Techniques*, **2332** (2002), 466–481.

[108] J. Hur and D. K. Noh, Attribute-based access control with efficient revocation in data outsourcing systems, *IEEE Transactions on Parallel and Distributed Systems*, **22** (2010), 1214–1221.

[109] V. Iovino and G. Persiano, Hidden-vector encryption with groups of prime order, In *International Conference on Pairing-Based Cryptography*, **5209** (2008), 75–88.

[110] J. Katz, A. Sahai and B. Waters, Predicate encryption supporting disjunctions, polynomial equations, and inner products, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **4965** (2008), 146–162.

[111] S. Kim, K. Lewi, A. Mandal, H. Montgomery, A. Roy and D. J. Wu, Function-hiding inner product encryption is practical, In *International Conference on Security and Cryptography for Networks*, **11035** (2018), 544–562.

[112] S. Kim, J. Kim and J. H. Seo, A new approach to practical function-private inner product encryption, *Theoret. Comput. Sci.*, **783** (2019), 22–40.

[113] C.-C. Lee, P.-S. Chung and M.-S. Hwang, A survey on attribute-based encryption schemes of access control in cloud environments, *IJ Network Security*, **15** (2013), 231–240.

[114] K. Lee, S. G. Choi, D. H. Lee, J. H. Park and M. Yung, Self-updatable encryption: Time constrained access control with hidden attributes and better efficiency, In *International Conference on the Theory and Application of Cryptology and Information Security*, **8269** (2013), 235–254.

[115] A. Lewko, T. Okamoto, A. Sahai, K. Takashima and B. Waters, Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **6110** (2010), 62–91.

[116] A. Lewko and B. Waters, New techniques for dual system encryption and fully secure HIBE with short ciphertexts, In *Theory of Cryptography Conference*, **5978** (2010), 455–479.

[117] A. Lewko and B. Waters, Decentralizing attribute-based encryption, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **6632** (2011), 568–588.

[118] A. Lewko and B. Waters, Unbounded HIBE and attribute-based encryption, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **6632** (2011), 547–567.

[119] J. Li, S. Hu, Y. Zhang and J. Han, A decentralized multi-authority ciphertext-policy attribute-based encryption with mediated obfuscation, *Soft Computing*, **24** (2020), 1869–1882.

[120] J. Li, Q. Yu and Y. Zhang, Hierarchical attribute based encryption with continuous leakage-resilience, *Information Sciences*, **484** (2019), 113–134.

[121] B. Libert and R. Ţiţiu, Multi-client functional encryption for linear functions in the standard model from LWE, In *International Conference on the Theory and Application of Cryptology and Information Security*, (2019), 520–551.

[122] H. Lin, Z. Cao, X. Liang and J. Shao, Secure threshold multi authority attribute based encryption without a central authority, *Inform. Sci.*, **180** (2010), 2618–2632.

[123] H. Lin, Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 PRGs, In *Annual International Cryptology Conference*, **10401** (2017), 599–629.

[124] H. Lin and S. Tessaro, Indistinguishability obfuscation from trilinear maps and block-wise local PRGs, In *Annual International Cryptology Conference*, **10401** (2017), 630–660.

[125] W. Liu, Q. Huang, X. Chen and H. Li, Efficient functional encryption for inner product with simulation-based security, *Cybersecurity*, **4** (2021), 1–13.

[126] Z. Liu, Z. Cao and D. S. Wong, Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on ebay, In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, (2013), 475–486.

[127] Z. Liu and D. S. Wong, Practical ciphertext-policy attribute-based encryption: Traitor tracing, revocation, and large universe, In *International Conference on Applied Cryptography and Network Security*, **9092** (2015), 127–146.

[128] Z. Liu and D. S. Wong, Traceable CP-ABE on prime order groups: Fully secure and fully collusion-resistant blackbox traceable, In *International Conference on Information and Communications Security*, **9543** (2015), 109–124.

[129] R. Longo, C. Marcolla and M. Sala, Key-policy multi-authority attribute-based encryption, In *International Conference on Algebraic Informatics*, **9270** (2015), 152–164.

[130] R. Longo, C. Marcolla and M. Sala, *Collaborative Multi-authority KP-ABE for Shorter Keys and Parameters*, International Conference on Algebraic Informatics, 2017, `https://eprint.iacr.org/2016/262`.

[131] F. Ma and M. Zhandry, The MMap strikes back: Obfuscation and new multilinear maps immune to CLT13 zeroizing attacks, In *Theory of Cryptography Conference*, **11240** (2018), 513–543.

[132] X. Ma, X. Wang and D. Lin, Anonymous identity-based encryption with identity recovery, In *Australasian Conference on Information Security and Privacy*, **10946** (2018), 360–375.

[133] A. J. Menezes, T. Okamoto and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory*, **39** (1993), 1639–1646.

[134] V. S. Miller, The Weil pairing, and its efficient calculation, *J. Cryptology*, **17** (2004), 235–261.

[135] A. Miyaji, M. Nakabayashi and S. Takano, New explicit conditions of elliptic curve traces for FR-reduction. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **84** (2001), 1234–1243.

[136] S. Müller, S. Katzenbeisser and C. Eckert, Distributed attribute-based encryption, In *International Conference on Information Security and Cryptology*, **5461** (2008), 20–36.

[137] D. Naccache, Secure and practical identity-based encryption, *IET Information Security*, **1** (2007), 59–64.

[138] M. Naveed, S. Agrawal, M. Prabhakaran, X. Wang, E. Ayday, J.-P. Hubaux and C. Gunter, Controlled functional encryption, In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, (2014), 1280–1291.

[139] J. Ning, Z. Cao, X. Dong, L. Wei and X. Lin, Large universe ciphertext-policy attribute-based encryption with white-box traceability, In *European Symposium on Research in Computer Security*, **8713** (2014), 55–72.

[140] T. Okamoto and K. Takashima, Homomorphic encryption and signatures from vector decomposition, In *International Conference on Pairing-Based Cryptography*, **5209** (2008), 57–74.

[141] T. Okamoto and K. Takashima, Hierarchical predicate encryption for inner-products, In *International Conference on the Theory and Application of Cryptology and Information Security*, **5912** (2009), 214–231.

[142] T. Okamoto and K. Takashima, Fully secure functional encryption with general relations from the decisional linear assumption, In *Annual Cryptology Conference*, **6223** (2010), 191–208.

[143] T. Okamoto and K. Takashima, Adaptively attribute-hiding (hierarchical) inner product encryption, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **7237** (2012), 591–608.

[144] T. Okamoto and K. Takashima, Fully secure unbounded inner-product and attribute-based encryption, In*International Conference on the Theory and Application of Cryptology and Information Security*, **7658** (2012), 349–366.

[145] T. Okamoto and K. Takashima, Efficient (hierarchical) inner-product encryption tightly reduced from the decisional linear assumption, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, **96** (2013), 42–52.

[146] A. O'Neill, *Definitional Issues in Functional Encryption*, Cryptology ePrint Archive, Report 2009/556, 2010, https://eprint.iacr.org/2010/556.

[147] R. Ostrovsky, A. Sahai and B. Waters, Attribute-based encryption with non-monotonic access structures, In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, (2007), 195–203.

[148] D. Page, N. P. Smart and F. Vercauteren, A comparison of MNT curves and supersingular curves, *Appl. Algebra Engrg. Comm. Comput.*, **17** (2006), 379–392.

[149] J. H. Park, Efficient hidden vector encryption for conjunctive queries on encrypted data, *IEEE Transactions on Knowledge and Data Engineering*, **23** (2010), 1483–1497.

[150] J. H. Park, Inner-product encryption under standard assumptions, *Des. Codes Cryptogr.*, **58** (2011), 235–257.

[151] J. H. Park, K. Lee, W. Susilo and D. H. Lee, Fully secure hidden vector encryption under standard assumptions, *Inform. Sci.*, **232** (2013), 188–207.

[152] J. Patarin and L. Goubin, Trapdoor one-way permutations and multivariate polynomials, In *International Conference on Information and Communications Security*, **1334** (1997), 356–368.

[153] C. Peikert, *Bonsai Trees (or, Arboriculture in Lattice-Based Cryptography)*, Cryptology ePrint Archive, Report 2009/359, 2009, https://eprint.iacr.org/2009/359.

[154] D. H. Phan and V. C. Trinh, Identity-based trace and revoke schemes, In *International Conference on Provable Security*, **6980** (2011), 204–221.

[155] Z. Qiao, S. Liang, S. Davis and H. Jiang, Survey of attribute based encryption, In *15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*, (2014), 1–6.

[156] Y. Rahulamathavan, S. Veluru, J. Han, F. Li, M. Rajarajan and R. Lu, User collusion avoidance scheme for privacy-preserving decentralized key-policy attribute-based encryption, *IEEE Trans. Comput.*, **65** (2016), 2939–2946.

[157] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, *J. ACM (JACM)*, **56** (2009), 1–40.

[158] K. Dey, S. K. Debnath, S. Mesnager and N. Kundu, Post-quantum secure inner product functional encryption using multivariate public key cryptography, *Mediterr. J. Math.*, **18** (2021).

[159] A. Sahai and H. Seyalioglu, Worry-free encryption: Functional encryption with public keys, In *Proceedings of the 17th ACM Conference on Computer and CVommunications Security*, (2010), 463–472.

[160] A. Sahai and B. Waters, Fuzzy identity-based encryption, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **3494** (2005), 457–473.

[161] S. Sedghi, P. V. Liesdonk, S. Nikova, P. Hartel and W. Jonker, Searching keywords with wildcan on encrypted data, In *International Conference on Security and Cryptography for Networks*, **6280** (2010), 138–153.

[162] A. Shamir, How to share a secret, *Comm. ACM*, **22** (1979), 612–613.

[163] A. Shamir, Identity-based cryptosystems and signature schemes, In *Workshop on the Theory and Application of Cryptographic Techniques*, **196** (1984), 47–53.

[164] E. Shen, E. Shi and B. Waters, Predicate privacy in encryption systems, In *Theory of Cryptography Conference*, **5444** (2009), 457–473.

[165] E. Shi and B. Waters, Delegating capabilities in predicate encryption systems, In *International Colloquium on Automata, Languages, and Programming*, **5126** (2008), 560–578.

[166] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Review*, **41** (1999), 303–332.

[167] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edition, Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.

[168] N. Soroush, V. Iovino, A. Rial, P. B. Roenne and P. Y. Ryan, Verifiable inner product encryption scheme, In *IACR International Conference on Public-Key Cryptography*, **12110** (2020), 65–94.

[169] K. Takashima, Efficiently computable distortion maps for supersingular curves, In *International Algorithmic Number Theory Symposium*, **5011** (2008), 88–101.

[170] C. Tang, D. Pei, Z. Liu and Y. He, *Non-Interactive and Information-Theoretic Secure Publicly Verifiable Secret Sharing*, Cryptology ePrint Archive, Report 2004/201, 2004, https://eprint.iacr.org/2004/201.

[171] Q. Tang and D. Ji, Verifiable attribute-based encryption, *IJ Network Security*, **10** (2010), 114–120.

[172] B. C. Tea, M. R. K. Ariffin and M. A. Asbullah, Identity-based encryption schemes–A review, *J. Multidisciplinary Engineering Science and Technology (JMEST)*, **6** (2019).

[173] J. Tomida, M. Abe and T. Okamoto, Efficient functional encryption for inner-product values with full-hiding security, In *International Conference on Information Security*, **9866** (2016), 408–425.

[174] J. Tomida and K. Takashima, Unbounded inner product functional encryption from bilinear maps, *Jpn. J. Ind. Appl. Math.*, **37** (2020), 723–779.

[175] T. van de Kamp, A. Peter and W. Jonker, A multi-authority approach to various predicate encryption types, *Des. Codes Cryptogr.*, **88** (2020), 363–390.

[176] G. Wang, Q. Liu and J. Wu, Hierarchical attribute-based encryption for fine-grained access control in cloud storage services, In *Proceedings of the 17th ACM Conference on Computer and Communications Security*, (2010), 735–737.

[177] B. Waters, Efficient identity-based encryption without random oracles, In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, **3494** (2005), 114–127.

[178] B. Waters, Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions, In *Annual International Cryptology Conference*, **5677** (2009), 619–636.

[179] B. Waters, Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization, In *International Workshop on Public Key Cryptography*, **6571** (2011), 53–70.

[180] H. Wee, Attribute-hiding predicate encryption in bilinear groups, revisited, In *Theory of Cryptography Conference*, **10677** (2017), 206–233.

[181] H. Wee, Functional encryption for quadratic functions from k-Lin, revisited, In *Theory of Cryptography Conference*, **12550** (2020), 210–228.

[182] P. Xu, J. Li, W. Wang and H. Jin, Anonymous identity-based broadcast encryption with constant decryption complexity and strong security, In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, (2016), 223–233.

[183] Y. Yang, X. Chen, H. Chen and X. Du, Improving privacy and security in decentraliz-
ing multi-authority attribute-based encryption in cloud computing, *IEEE Access*, **6** (2018),
18009–18021.

[184] M. Zhang, B. Yang and T. Takagi, Bounded leakage-resilient functional encryption with
hidden vector predicate, *Computer Journal*, **56** (2013), 464–477.

[185] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li and D. Zheng, Attribute-based encryption for
cloud computing access control: A survey, *ACM Computing Surveys (CSUR)*, **53** (2020),
1–41.

[186] Q. Zhao, Q. Zeng and X. Liu, Improved construction for inner product functional encryption,
Security and Communication Networks, **2018** (2018).

[187] Q. Zhao, Q. Zeng, X. Liu and H. Xu, Simulation-based security of function-hiding inner
product encryption, *Sci. China Inf. Sci.*, **61** (2018), 1–3.

E-mail address: {carla.mascia,massimiliano.sala,irene.villa}@unitn.it