Functional Encryption for Quadratic Functions, and Applications to Predicate Encryption

Romain Gay
ENS, CNRS, INRIA, and PSL, Paris, France
rgay@di.ens.fr

Abstract. We present a functional encryption scheme based on standard assumptions where ciphertexts are associated with a tuple of values $(x_1, \ldots, x_n) \in \mathbb{Z}_p^n$, secret keys are associated with a degree-two polynomial, and the decryption of a ciphertext $\mathsf{ct}_{(x_1,\ldots,x_n)\in\mathbb{Z}_p^n}$ with a secret key $\mathsf{sk}_{P\in\mathbb{Z}_p[X_1,\ldots,X_n],\mathsf{deg}(P)\leq 2}$ recovers $P(x_1, \ldots, x_n)$, where the ciphertext contains only $O(n)$ group elements. Our scheme, which achieves selective security based on pairings, also yields a new predicate encryption scheme that supports degree-two polynomial evaluation, generalizing both [26] and [10].

1 Introduction

Functional Encryption [11](in short: FE) is a general paradigm that allows to generate restricted decryption keys, that let users learn specific functions of the encrypted data, and nothing else. Namely, ciphertexts ct_x are associated with an attribute x, secret keys sk_f are associated with a function f, and the decryption of ct_x with sk_f allows to recover $f(x)$, and nothing more. In particular, ct_x does not leak its underlying attribute x. The scheme must be resistant to any collusion of secret keys sk_f for different functions f: such group of secret keys should not learn anything more than the information leaked by each key sk_f, individually. This security property makes FE schemes both hard to build and extremely useful, provided the class of function they handle is large. In fact, combining the results of [8, 4, 5] proves that an FE for sufficiently general functions[1] gives a construction for the almighty Indistinguishability Obfuscation for circuits [20]. Perhaps unsurprisingly given the versatility of these cryptographic notions, we do not know how to implement them based on standard assumptions, let alone efficient. Instead, another approach consider specific classes of functions, and give efficient constructions, based on standard assumptions. This is the case of Predicate Encryption [26](in short: PE), where ciphertexts are associated with a plaintext m and an attribute x, and secret keys are associated with a function f such that $f(m, x) = m$ if and only if $\mathsf{P}(x) = 1$, where P is a boolean predicate (note that these are stronger that attribute-based encryption [33, 24] since a ciphertext should not reveal its attribute x). More recently, [1, 3] build simple functional encryption for the inner product functionality, namely, where ciphertexts $\mathsf{ct}_{\mathbf{x}}$ are associated with vectors $\mathbf{x}$, secret keys are associated with vectors $\mathbf{y}$ of same dimension, and the decryption of $\mathsf{ct}_{\mathbf{x}}$ with $\mathsf{sk}_{\mathbf{y}}$ recovers the inner product of $\mathbf{x}$ and $\mathbf{y}$. To this date, boolean predicates and inner product are the only functionalities that we know how to build from standard assumptions.

[1] The FE scheme must support the evaluations of three weak PRF and simple, finite operations.

Our contributions.

We build the first FE scheme based on a standard assumption that supports a functionality beyond inner product, or predicates. In our scheme, ciphertexts are associated with a set of values, and secret keys are associated with a degree-two polynomial. This way, the decryption of a ciphertext $\mathsf{ct}_{(x_1,\ldots,x_n)\in\mathbb{Z}_p^n}$ with a secret key $\mathsf{sk}_{P\in\mathbb{Z}_p[X_1,\ldots,X_n],\deg(P)\leq 2}$ recovers $P(x_1,\ldots,x_n)$. The ciphertext size is $O(n)$ group elements, improving upon [1, 3], which would require $O(n^2)$ group elements, since they build an FE scheme for inner product. This implies new PE schemes that satisfy a so-called attribute-hiding property, that is, ciphertexts are associated with a set of values and a plaintext, secret keys are associated with a degree-two polynomial, and the decryption of a ciphertext $\mathsf{ct}_{(x_1,\ldots,x_n)\in\mathbb{Z}_p^n}$ with a secret key $\mathsf{sk}_{P\in\mathbb{Z}_p[X_1,\ldots,X_n],\ \deg(P)\leq 2}$ recovers the plaintext if, and only if, $P(x_1,\ldots,x_n)=1$. The attribute-hiding property refers to the fact that $\mathsf{ct}_{(x_1,\ldots,x_n)\in\mathbb{Z}_p^n}$ leaks no information on its attribute $(x_1,\ldots,x_n)$, beyond the inherent leakage of the boolean value $P(x_1,\ldots,x_n)=1$. Again, this is done with ciphertexts of $O(n)$ group elements, instead of $O(n^2)$ when using [26], which build an Inner Product Encryption (where the predicate is defined by a degree-one polynomial). Both our FE scheme and PE scheme are proved selectively secure under the Matrix Diffie-Hellman assumption [19], which generalizes standard assumptions such as DLIN or k-Lin for $k\geq 1$, and the 3-pddh assumption [10].

Comparison with prior works.

Prior PE schemes based on standard assumptions exist for Identity-Based Encryption [13, 2, 9, 7, 14, 38] (in this context, the attribute-hiding property is referred to as anonymity of the IBE), Inner Product Encryption [26, 31, 28, 32, 15, 17], and comparison [10, 12, 21], namely, when ciphertexts and secret keys are associated with values, and the secret-key $\mathsf{sk}_{y\in\mathbb{Z}_p}$ decrypts the ciphertext $\mathsf{ct}_{x\in\mathbb{Z}_p}$ if, and only if, $y\geq x$ (here we only cite works that are secure in the standard model, under static assumptions). IPE is the most expressive of these three, since the other predicates can be efficiently reduced to IP. The PE we build is even more expressive, since it allows to define predicate by degree-two polynomials. Note that there also exists lattice-based attribute-hiding PE for all circuits [23], or PE for comparison with $O(\log n)$ group elements per ciphertext [35, 22]. However, these PE are attribute-hiding in a weaker sense. In fact, in these so-called weakly attribute-hiding PE, ciphertexts can reveal their attribute if some secret keys that decrypt them are known (see Remark 1 for more details on the difference between weakly and fully attribute-hiding PE).

Technical overview.

The difficulty is to have ciphertexts $\mathsf{ct}_{(x_1,\ldots,x_n)}$ of $O(n)$ group elements, that must hide their attribute $(x_1,\ldots,x_n)\in\mathbb{Z}_p^n$, but still contain enough informations to recover the n^2 values $x_i\cdot x_j$ for $i,j\in[n]$. To ensure the attribute is hidden, the ciphertext will contain an encryption of each value x_i. Since we want to multiply together these encryptions to compute products $x_i\cdot x_j$, and since these encryption are composed of group elements, we require a pairing $e:\mathbb{G}_1\times\mathbb{G}_2\to\mathbb{G}_T$, where $\mathbb{G}_1$, $\mathbb{G}_2$, and $\mathbb{G}_T$ are additively written, prime-order groups. Namely, decryption pairs encrypted values in $\mathbb{G}_1$ with encrypted values in $\mathbb{G}_2$. For this reason, it makes sense to re-write the function as: $\mathcal{X}:=\mathbb{Z}_p^n\times\mathbb{Z}_p^m$, $\mathcal{K}:=\mathbb{Z}_p^{n\times m}$, and for all $(\mathbf{x},\mathbf{y})\in\mathcal{X}$, $\mathbf{M}\in\mathcal{K}$,

$$F((\mathbf{x},\mathbf{y}),\mathbf{M})=\mathbf{x}^\top\mathbf{M}\mathbf{y}=\sum_{i\in[n],j\in[m]}m_{i,j}x_iy_j.$$

Private-key, single-ciphertext secure FE. Our starting point is a private-key FE that is only secure for a single-ciphertext:

$$\mathsf{ct}_{\mathbf{x},\mathbf{y}} := \{[\mathbf{A}\mathbf{r}_i + \mathbf{b}^\perp x_i]_1\}_{i\in[n]}, \{[\mathbf{B}\mathbf{s}_j + \mathbf{a}^\perp y_j]_2\}_{j\in[m]} \text{ and } \mathsf{sk}_{\mathbf{M}} := [\sum_{i,j} m_{i,j}\mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_j]_T,$$

where we rely on implicit representation notation [19] for group elements : for a fixed generator P_s of $\mathbb{G}_s$ and for a matrix $\mathbf{A} \in \mathbb{Z}_p^{n\times t}$, we define $[\mathbf{A}]_s := \mathbf{A}P_s \in \mathbb{G}_s^{n\times t}$ where multiplication is done component-wise, with $s \in \{1, 2, T\}$. Here $(\mathbf{A}|\mathbf{b}^\perp)$ and $(\mathbf{B}|\mathbf{a}^\perp)$ are bases of $\mathbb{Z}_p^{k+1}$ such that $\mathbf{A}^\top\mathbf{a}^\perp = \mathbf{B}^\top\mathbf{b}^\perp = \mathbf{0}$, à la [16]. The vectors $[\mathbf{A}\mathbf{r}_i]_1$ and $[\mathbf{B}\mathbf{s}_j]_2$ for $i \in [n], j \in [m]$, $\mathbf{a}^\perp$ and $\mathbf{b}^\perp$ are part of a master secret key, used to (deterministically) generate $\mathsf{ct}_{\mathbf{x},\mathbf{y}}$ and $\mathsf{sk}_{\mathbf{M}}$. Correctness follows from the orthogonal property: decryption computes $\sum_{i,j} m_{i,j} e([\mathbf{A}\mathbf{r}_i + \mathbf{b}^\perp x_i]_1^\top, [\mathbf{B}\mathbf{s}_j + \mathbf{a}^\perp y_j]_2) = \mathsf{sk}_{\mathbf{M}} + (\mathbf{b}^\perp)^\top\mathbf{a}^\perp \cdot [F((\mathbf{x},\mathbf{y}),\mathbf{M})]_T$ which is equal to $\mathsf{sk}_{\mathbf{M}}$ if, and only if, $F((\mathbf{x},\mathbf{y}),\mathbf{M}) = 0$. Security relies on the $\mathcal{D}_k$-mddh Assumption [19], which stipulates that given $[\mathbf{A}]_1$ drawn from a matrix distribution $\mathcal{D}_k$ over $\mathbb{Z}_p^{(k+1)\times k}$,

$$[\mathbf{A}\mathbf{r}]_1 \approx_c [\mathbf{A}\mathbf{r} + \mathbf{b}^\perp]_1 \text{ and } [\mathbf{B}\mathbf{s}]_1 \approx_c [\mathbf{B}\mathbf{s} + \mathbf{a}^\perp]_1,$$

where $\mathbf{r}, \mathbf{s} \leftarrow_R \mathbb{Z}_p^k$. This allows to change $\mathsf{ct}_{\mathbf{x}^0,\mathbf{y}^0}$ into $\mathsf{ct}_{\mathbf{x}^1,\mathbf{y}^1}$, but creates an extra term $\left[\sum_{i,j} m_{i,j}x_i^1 y_j^1 - \sum_{i,j} m_{i,j}x_i^0 y_j^0\right]_T$ in the secret keys $\mathsf{sk}_{\mathbf{M}}$. We conclude the proof using the fact that for all $\mathbf{M}$ queried to KeyGen, $F((\mathbf{x}^0,\mathbf{y}^0),\mathbf{M}) = F((\mathbf{x}^1,\mathbf{y}^1),\mathbf{M})$, as required by the security definition for FE (see Section 2.4.2 for the definition of FE), which cancels out the extra term in all secret keys.

Public-key FE. Going from one to many challenge ciphertexts poses three problems.

Problem 1. Generating $[\mathbf{A}\mathbf{r}_i + \mathbf{b}^\perp x_i^j]_1$ for a fixed $i \in [n]$ but different j requires to know $\mathbf{a}^\perp$, which prevent using MDDH on $[\mathbf{A}]_1$. The same problem holds relative to $[\mathbf{B}]_2$ and $\mathbf{b}^\perp$. In fact, this is even more stringent in the public-key setting, since $[\mathbf{a}^\perp]_2$ and $[\mathbf{b}^\perp]_1$ would need to be part of the public key.

Problem 2. There are mix and match attacks, where some part of a challenge ciphertext is used with a part of another ciphertext to break the scheme. For instance in the case $n = m = 1$, pairing the part $[\mathbf{A}\mathbf{r}_1 + \mathbf{b}^\perp x^0]_1$ of ciphertext ct_{x^0,y^0} with the part $[\mathbf{B}\mathbf{s}_1 + \mathbf{a}^\perp y^1]_1$ of ciphertext ct_{x^1,y^1}, together with the secret key $\mathsf{sk}_{\mathbf{M}} := [\mathbf{r}_1^\top\mathbf{A}^\top\mathbf{B}\mathbf{s}_1]_T$ for $\mathbf{M} = 1$, yields the value $[x^0 \cdot y^1]_T$ where only the values $[x^0 \cdot y^0]_T$ and $[x^1 \cdot y^1]_T$ should leak.

Problem 3. In the public-key setting, the secret keys $\mathsf{sk}_{\mathbf{M}}$ for all $\mathbf{M}$ are computable efficiently from the public key that contains the vectors $[\mathbf{A}\mathbf{r}_i]_1$, $[\mathbf{B}\mathbf{s}_j]_2$.

Solution to problem 1. We add an extra dimension, namely, we use bases $\left(\begin{array}{c|c} \mathbf{A}|\mathbf{b}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)$ and $\left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)$ where the extra dimension will be used for correctness, while $(\mathbf{A}|\mathbf{b}^\perp)$ and $(\mathbf{B}|\mathbf{a}^\perp)$ will be used for security (using the mddh assumption, since $\mathbf{a}^\perp$ and $\mathbf{b}^\perp$ are not part of the public key anymore).

Solution to problem 2. The encryption randomizes the bases

$$\left(\begin{array}{c|c} \mathbf{A}|\mathbf{b}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right) \text{ and } \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)$$

into

$$\mathbf{W}^{-1}\left(\begin{array}{c|c}\mathbf{A}|\mathbf{b}^{\perp} & 0\\ \hline \mathbf{0} & 1\end{array}\right) \text{ and } \mathbf{W}^{\top}\left(\begin{array}{c|c}\mathbf{B}|\mathbf{a}^{\perp} & 0\\ \hline \mathbf{0} & 1\end{array}\right)$$

for $\mathbf{W} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$ a random invertible matrix. This "glues" the components of a ciphertext that are in G_1 to those that are in G_2.

Solution to problem 3. we generate secret keys in $\mathbb{G}_2$ instead of $\mathbb{G}_T$, namely

$$\mathsf{sk}_{\mathbf{M}} := [\sum_{i,j} m_{i,j}\mathbf{r}_i^{\top}\mathbf{A}^{\top}\mathbf{B}\mathbf{s}_j]_2.$$

We also randomize the ciphertexts, which contain $[\mathbf{A}\mathbf{r}_i \cdot \gamma]_1$ and $[\mathbf{B}\mathbf{s}_j \cdot \sigma]_2$, where $\gamma, \sigma \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ are the same for all $i \in [n]$, and $j \in [m]$, but fresh for each ciphertext. The ciphertexts also contain $[\gamma \cdot \sigma]_1$, for correctness. This way, decryption gets $[F((\mathbf{x},\mathbf{y}),\mathbf{M})]_T + [\gamma\sigma \cdot \sum_{i,j} m_{i,j}\mathbf{r}_i^{\top}\mathbf{A}^{\top}\mathbf{B}\mathbf{s}_j]_T$, where the second term of the sum is $e([\gamma\sigma]_1, \mathsf{sk}_{\mathbf{M}})$. Including this "quadratic information" $[\gamma \cdot \sigma]_2$ inside the ciphertexts is similar to the techniques used originally in [10], and in follow up [12, 21]. The similarity with these schemes ends here: we need significantly new techniques to achieve general quadratic functions (they focus on a particular case of quadratic function). A more detailed comparison between our work and these papers is provided in the Discussion paragraph.

New problem 4. Computing secret keys in the group $\mathbb{G}_2$ instead of the target group $\mathbb{G}_T$, poses a new problem when using a type 3 pairing (where there are no efficient isomorphism between $\mathbb{G}_1$ and $\mathbb{G}_2$), namely, how can we compute $[\mathbf{A}]_2$ and use the MDDH assumption on $[\mathbf{A}]_1$, in $\mathbb{G}_1$? Note that this problem does not arises in type 1 pairing (when $\mathbb{G}_1 = \mathbb{G}_2$), but this is a less efficient setting that type 3 pairing, as demonstrated in [25].

Solution to problem 4. We secret share the secret keys in both $\mathbb{G}_1$ and $\mathbb{G}_2$, allowing to generate them only $([\mathbf{A}]_1, [\mathbf{B}]_1)$ or $([\mathbf{A}]_2, [\mathbf{B}]_2)$, but not both. Namely, $\mathsf{KeyGen}(\mathsf{msk}, \mathbf{M})$ computes $K := [\sum_{i,j} m_{i,j}\mathbf{r}_i^{\top}\mathbf{A}^{\top}\mathbf{B}\mathbf{s}_j]_1 - [u]_1$ and $\widehat{K} := [u]_2$, for $u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ that is freshly picked for each secret key. This way, there is essentially two to compute secret keys: by computing a meaningful value in $\mathbb{G}_1$, and a random value in $\mathbb{G}_2$, or vice versa. Finally, for correctness, the ciphertexts include the values $[\gamma \cdot \sigma]_1$ and $[\gamma \cdot \sigma]_2$ for $\gamma, \sigma \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, and the decryption can cancel out the second term of the sum $[F((\mathbf{x},\mathbf{y}),\mathbf{M})]_T + [\gamma\sigma \cdot \sum_{i,j} m_{i,j}\mathbf{r}_i^{\top}\mathbf{A}^{\top}\mathbf{B}\mathbf{s}_j]_T$ by computing $e([\gamma\sigma]_1, \widehat{K}) + e(K, [\gamma\sigma]_2)$.

Combining the solutions to problems 1 to 4, we obtain:

$$\mathsf{ct}_{\mathbf{x},\mathbf{y}} := \left(\left\{\left[\begin{pmatrix}\mathbf{A}\mathbf{r}_i \cdot \gamma\\ x_i\end{pmatrix}^{\top}\mathbf{W}^{-1}\right]_1\right\}_{i\in[n]}, \left\{\left[\mathbf{W}\begin{pmatrix}\mathbf{B}\mathbf{s}_j \cdot \sigma\\ y_j\end{pmatrix}\right]_2\right\}_{j\in[m]}, [\gamma \cdot \sigma]_1, [\gamma \cdot \sigma]_2\right)$$

where $\mathbf{W} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$ and $\gamma, \sigma \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ are freshly picked for each ciphertext, and

$$\mathsf{sk}_{\mathbf{M}} := (K, \widehat{K}) \text{ where } K := [\sum_{i,j} m_{i,j}\mathbf{r}_i^{\top}\mathbf{A}^{\top}\mathbf{B}\mathbf{s}_j]_1 - [u]_1 \text{ and } \widehat{K} := [u]_2.$$

where $u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ is freshly picked for each secret key.

Then, to get back the value $F((\mathbf{x},\mathbf{y}),\mathbf{M})$ in $\mathbb{Z}_p$ (and not only in $\mathbb{G}_T$), we need to solve discrete log in $\mathbb{G}_T$, for instance using a look-up table when the output of F is small, as done in previous FE such as [1, 3].

Discussion.

The scheme described above is identically distributed to:

$$\mathsf{ct}_{\mathbf{x},\mathbf{y}} := \left(\left\{ \left[\begin{pmatrix} \mathbf{r}_i \cdot \gamma \\ x_i \end{pmatrix}^\top \mathbf{W}^{-1} \right]_1 \right\}_{i \in [n]}, \left\{ \left[\mathbf{W} \begin{pmatrix} \mathbf{s}_j \cdot \sigma \\ y_j \end{pmatrix} \right]_2 \right\}_{j \in [m]}, [\gamma \cdot \sigma]_1, [\gamma \cdot \sigma]_2 \right)$$

where $\mathbf{r}_i, \mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$,

$$\mathsf{sk}_{\mathbf{M}} := (K, \widehat{K}) \text{ where } K := [\sum_{i,j} m_{i,j} \mathbf{r}_i^\top \mathbf{s}_j]_1 - [u]_1 \text{ and } \widehat{K} := [u]_2.$$

This is reminiscent from constructions based on Dual Pairing Vector Space, originally introduced in [30], and later used in [31, 27, 17] in the context of attribute-based encryption, and in [18, 36] in the context of FE for inner product, with the crucial difference the all these previous constructions do not include quadratic terms of the form $[\mathbf{r}_i^\top \mathbf{s}_j]_2$. The technical difficulty is to achieve security even when these terms are leaked in the secret keys. More specifically, these previous approaches use a security paradigm called Dual System Encryption, introduced by [37], where the security proof uses a hybrid argument over all secret keys, leaving the distribution of the public key identical. This is different from our proof, which changes the distribution of the public and secret keys, and whose security loss does not depend on the number of queried secret keys.

Finally, our approach differs from [10] and follow-up works [12, 21] in that these previous works focus an a particular case of quadratic function, namely, the predicate comparison (see Section 4), for which it is enough to consider vectors of the form: $[\mathbf{A}\mathbf{r}_i + x_i \mathbf{b}^\perp]_1, [\mathbf{B}\mathbf{s}_j + y_j \mathbf{a}^\perp]_2$, where x_i and y_j are either 0, either some random value (fixed at setup time, and identical for all ciphertexts and secret keys), or the vectors are just some "trash" random vector, i.e that do not contain any useful information.In this case, the problem 2. pointed out previously does not arise. We introduce new techniques to solve problem 2., thereby generalizing the aforementioned works to any quadratic functions.

Concurrent and Independent work.

In concurrent and independent work, Lin [29], and Ananth and Sahai [6] present constructions of *private-key* functional encryption schemes for degree-D polynomials based on D-linear maps. As a special case for $D = 2$, these schemes support quadratic polynomials from bilinear maps, as ours. Also, in terms of security, the construction of Lin is proven selectively secure based on the SXDH assumption, while the scheme of Ananth and Sahai is selectively secure based on ad-hoc assumptions that are justified in the multilinear group model. In comparison to these works, our schemes have the advantage of working in the (arguably more challenging) *public key* setting.

Road map.

We first give the necessary notations and preliminaries in Section 2. Then, following the technical overview, we first give a private-key functional encryption scheme that is only secure when there is one challenge ciphertext in Section 3.1, and we give our public-key functional encryption in Section 3.2. In Section 4, we show how this gives a new PE that supports degree-two polynomial evaluation, and how this applies to other interesting predicates, such as comparison.

2 Preliminaries

2.1 Notations

For a finite set S, $|S|$ denotes its cardinality, and we denote by $s \leftarrow_{\mathrm{R}} S$ the fact that s is picked uniformly at random from S. By PPT, we denote a probabilistic polynomial-time algorithm. We denote by λ the security parameter, and by $\mathsf{negl}(\cdot)$ any negligible function of λ. We denote vectors $\vec{x} = (x_i)$ and matrices $\mathbf{A} = (a_{i,j})$ in bold. For any prime p and any matrix $\mathbf{A} \in \mathbb{Z}_p^{n \times m}$ with $n \geq m$, we denote by $\mathsf{orth}(\mathbf{A}) := \{\mathbf{a}^\perp \in \mathbb{Z}_p^n : \mathbf{A}^\top \mathbf{a}^\perp = \mathbf{0}\}$. For all square matrices $\mathbf{A} \in \mathbb{Z}_p^{n \times n}$, we denote by $\det(\mathbf{A})$ the determinant of $\mathbf{A}$. For any $n \in \mathbb{N}^*$, we denote by GL_n the general linear group of degree n, that is, the set of all $n \times n$ invertible matrices over $\mathbb{Z}_p$.

2.2 Pairing groups

Let GGen be a probabilistic polynomial time (PPT) algorithm that on input the security parameter 1^λ, returns a description $\mathcal{PG} = (p, \mathbb{G}_1, \mathbb{G}_2, P_1, P_2, \mathbb{G}_T, e)$ of pairing groups where $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$ are cyclic group of order p for a λ-bit prime p, P_1, P_2 are generators of $\mathbb{G}_1$, $\mathbb{G}_2$, respectively, and $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ is an efficiently computable (non-degenerate) bilinear map. Define $P_T := e(P_1, P_2)$, which is a generator of $\mathbb{G}_T$. We use implicit representation of group elements: for $a \in \mathbb{Z}_p$, define $[a]_s = aP_s \in \mathbb{G}_s$ as the implicit representation of a in $\mathbb{G}_s$, for $s \in \{1, 2, T\}$. Given $[a]_1$ and $[b]_2$, one can efficiently compute $[ab]_T$ using the pairing e. For two matrices $\mathbf{A}$, $\mathbf{B}$ with matching dimensions define $e([\mathbf{A}]_1, [\mathbf{B}]_2) := [\mathbf{AB}]_T$.

2.3 Complexity assumptions

We recall the definitions of the Matrix Decision Diffie-Hellman (mddh) Assumption [19].

Definition 1 (*Matrix Distribution*)

Let $k \in \mathbb{N}^*$. We call $\mathcal{D}_k$ a matrix distribution if it outputs, in polynomial time, matrices in $\mathbb{Z}_p^{(k+1)\times k}$ of full rank k, and satisfying the following property:

Property 1

$$\Pr[\mathsf{orth}(\mathbf{A}) \subseteq \mathsf{span}(\mathbf{B})] = \frac{1}{\Omega(p)},$$

where $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$.

Without loss of generality, we assume the first k rows of $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$ form an invertible matrix. Note that the basis property is not explicit in [19], but, as noted in [16, Lemma 1 (basis lemma)], all examples of matrix distribution presented in [19, Section 3.4], namely $\mathcal{U}_k$, $\mathcal{L}_k$, $\mathcal{SC}_k$, $\mathcal{C}_k$ and $\mathcal{IL}_k$, satisfy this property.

The $\mathcal{D}_k$-Matrix Diffie-Hellman problem in $\mathbb{G}_s$ for $s \in \{1, 2, T\}$ is to distinguish the two distributions $([\mathbf{A}]_s, [\mathbf{Aw}]_s)$ and $([\mathbf{A}]_s, [\mathbf{u}]_s)$ where $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, $\mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and $\mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$.

Definition 2 ($\mathcal{D}_k$-*Matrix Diffie-Hellman Assumption* $\mathcal{D}_k$-mddh)

Let $\mathcal{D}_k$ be a matrix distribution. We say that the $\mathcal{D}_k$-Matrix Diffie-Hellman ($\mathcal{D}_k$-mddh) Assumption holds relative to GGen in $\mathbb{G}_s$, for $s \in \{1, 2, T\}$, if for all PPT adversaries $\mathcal{A}$,

$$\mathbf{Adv}^{\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathbb{G}_s,\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(\mathcal{PG}, [\mathbf{A}]_s, [\mathbf{Aw}]_s) = 1] - \Pr[\mathcal{A}(\mathcal{PG}, [\mathbf{A}]_s, [\mathbf{u}]_s) = 1]| = \mathsf{negl}(\lambda),$$

where the probability is taken over $\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k, \mathbf{w} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k, \mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$.

For each $k \geq 1$, [19] specifies distributions ($\mathcal{U}_k$, $\mathcal{L}_k$, $\mathcal{SC}_k$, $\mathcal{C}_k$ and $\mathcal{IL}_k$) over $\mathbb{Z}_p^{(k+1)\times k}$ such that the corresponding $\mathcal{D}_k$-mddh assumptions are generically secure in bilinear groups and form a hierarchy of increasingly weaker assumptions. $\mathcal{L}_k$-mddh is the well known k-Linear Assumption k-Lin with 1-Lin = DDH.

Let $Q \geq 1$. For $\mathbf{W} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k\times Q}, \mathbf{U} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times Q}$, we consider the Q-fold $\mathcal{D}_k$-mddh Assumption which consists in distinguishing the distributions $([\mathbf{A}], [\mathbf{AW}])$ from $([\mathbf{A}], [\mathbf{U}])$. That is, a challenge for the Q-fold $\mathcal{D}_k$-mddh Assumption consists of Q independent challenges of the $\mathcal{D}_k$-mddh Assumption (with the same $\mathbf{A}$ but different randomness $\mathbf{w}$). In [19] it is shown that the two problems are equivalent.

Lemma 1 (*Random self-reducibility of $\mathcal{U}_{\ell,k}$-mddh, [19]*)

Let $k, Q \in \mathbb{N}$, and $s \in \{1, 2, T\}$. For any PPT adversary $\mathcal{A}$, there exists a PPT adversary $\mathcal{B}$ such that

$$\mathbf{Adv}^{Q\text{-}\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_s,\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_s,\mathcal{B}}(\lambda) + \frac{1}{p-1}$$

where $\mathbf{Adv}^{Q\text{-}\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_s,\mathcal{A}}(\lambda) := |\Pr[\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_s, [\mathbf{AW}]_s) = 1] - \Pr[\mathcal{B}(\mathcal{PG}, [\mathbf{A}]_s, [\mathbf{U}]_s) = 1]|$ and the probability is taken over $\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{U}_k, \mathbf{W} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{k\times Q}, \mathbf{U} \leftarrow_{\mathrm{R}} \mathbb{Z}_q^{(k+1)\times Q}$.

We also recall the definition of 3-party Decision Diffie-Hellman (3-pddh) Assumption introduced in [10]. We give a variant in the asymmetric-pairing setting.

Definition 3 (*3-party Decision Diffie-Hellman Assumption* 3-pddh)

We say that the 3-party Decision Diffie-Hellman Assumption (3-pddh) Assumption holds relative to GGen if for all PPT adversaries $\mathcal{A}$,

$$\begin{aligned}\mathbf{Adv}^{3-\mathsf{pddh}}_{\mathsf{GGen},\mathcal{A}}(\lambda) := |&\Pr[\mathcal{A}(\mathcal{PG}, [a]_1, [b]_2, [c]_1, [c]_2, [abc]_1) = 1] \\ &- \Pr[\mathcal{A}(\mathcal{PG}, [a]_1, [b]_2, [c]_1, [c]_2, [d]_1) = 1]| \\ &= \mathsf{negl}(\lambda)\end{aligned}$$

where the probability is taken over $\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $a, b, c, d \leftarrow_{\mathrm{R}} \mathbb{Z}_p$.

2.4 Functional Encryption

A functional encryption scheme for a function $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ consists of four algorithms (Setup, Enc, KeyGen, Dec):

- $\mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{K}, \mathcal{Y}) \to (\mathsf{pk}, \mathsf{msk}, \mathsf{ek})$. The setup algorithm gets as input the security parameter λ, the key space $\mathcal{K}$, the plaintext space $\mathcal{X}$, the output space $\mathcal{Y}$, and outputs the public key pk, the master key msk and the encryption key ek. In a private-key scheme, $\mathsf{ek} := \mathsf{msk}$, whereas $\mathsf{ek} := \emptyset$ in a public-key scheme.
- $\mathsf{Enc}(\mathsf{pk}, \mathsf{ek}, x) \to \mathsf{ct}_x$. The encryption algorithm gets as input the public key pk, the encryption key ek, and a plaintext $x \in \mathcal{X}$. It outputs a ciphertext ct_x.
- $\mathsf{KeyGen}(\mathsf{pk}, \mathsf{msk}, k) \to \mathsf{sk}_k$. The key generation algorithm gets as input msk and a key $k \in \mathcal{K}$. It outputs a secret key sk_k.
- $\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_k, k, \mathsf{ct}_x) \to y$. The decryption algorithm gets as input sk_k, the associated key k, and ct_x. It outputs $y \in \mathcal{Y}$.

2.4.1 Correctness.

We require that for all $(k, x) \in \mathcal{K} \times \mathcal{X}$,

$$\Pr[\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_k, k, \mathsf{Enc}(\mathsf{pk}, \mathsf{ek}, x)) = F(k, x)] = 1,$$

where the probability is taken over $(\mathsf{pk}, \mathsf{msk}, \mathsf{ek}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{K}, \mathcal{Y})$, $\mathsf{sk}_k \leftarrow \mathsf{KeyGen}(\mathsf{pk}, \mathsf{msk}, k)$, and the coins of Enc.

2.4.2 Security definition.

For a stateful adversary $\mathcal{A}$ and a functional encryption scheme FE, we define the advantage function

$$\mathsf{Adv}^{\mathsf{FE}}_{\mathcal{A}}(\lambda) := \Pr\left[b = b' : \begin{array}{l} \mathsf{state} \leftarrow \mathcal{A}^{\mathsf{SetupO}(\cdot,\cdot)}; \\ b' \leftarrow \mathcal{A}^{\mathsf{KeyGenO}(\cdot)}(\mathsf{state}) \end{array}\right] - \frac{1}{2}$$

where SetupO, on input $(x^{(0)} \in \mathcal{X}, x^{(1)} \in \mathcal{X})$, computes $(\mathsf{pk}, \mathsf{msk}, \mathsf{ek}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{K})$, picks $b \leftarrow_{\mathrm{R}} \{0, 1\}$, and returns $(\mathsf{pk}, \mathsf{Enc}(\mathsf{ek}, \mathsf{pk}, x^{(b)})$; $\mathsf{KeyGenO}$, on input $k \in \mathcal{K}$, returns $\mathsf{KeyGen}(\mathsf{msk}, k)$; with the requirement that SetupO is called only once at the beginning of the game, and that all queries $k \in \mathcal{K}$ that $\mathcal{A}$ makes to $\mathsf{KeyGenO}(\cdot)$ satisfy $F(k, x^{(0)}) = F(k, x^{(1)})$. FE is said to be *selectively secure*, if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}^{\mathsf{FE}}_{\mathcal{A}}(\lambda) = \mathsf{negl}(\lambda)$. Note that in the private-key setting, this corresponds to single-ciphertext security, since the adversary only gets to see one challenge ciphertext (and contrary to the public-key setting, it cannot generate ciphertext by itself without ek).

2.5 Predicate Encryption

An predicate encryption (PE) scheme for a predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0, 1\}$ consists of four algorithms $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{KeyGen}, \mathsf{Dec})$:

- $\mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{Y}, \mathcal{M}) \to (\mathsf{pk}, \mathsf{msk})$. The setup algorithm gets as input the security parameter λ, the attribute universe $\mathcal{X}$, the predicate universe $\mathcal{Y}$, the message space $\mathcal{M}$ and outputs the public parameter pk, and the master key msk.
- $\mathsf{Enc}(\mathsf{pk}, x, M) \to \mathsf{ct}_x$. The encryption algorithm gets as input pk, an attribute $x \in \mathcal{X}$ and a message $M \in \mathcal{M}$. It outputs a ciphertext ct_x. Note that x is public given ct_x.
- $\mathsf{KeyGen}(\mathsf{pk}, \mathsf{msk}, y) \to \mathsf{sk}_y$. The key generation algorithm gets as input msk and a value $y \in \mathcal{Y}$. It outputs a secret key sk_y.
- $\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_y, y, \mathsf{ct}_x) \to M$. The decryption algorithm gets as input sk_y, the associated attribute y, and ct_x such that $\mathsf{P}(x, y) = 1$. It outputs a message M.

2.5.1 Correctness.

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

$$\Pr[\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_y, y, \mathsf{Enc}(\mathsf{pk}, x, M)) = M] = 1,$$

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

2.5.2 Security definition.

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

$$\mathsf{Adv}^{\mathsf{PE}}_{\mathcal{A}}(\lambda) := \Pr\left[b = b' : \begin{array}{l} \mathsf{state} \leftarrow \mathcal{A}^{\mathsf{SetupO}(\cdot,\cdot,\cdot,\cdot)}; \\ b' \leftarrow \mathcal{A}^{\mathsf{KeyGenO}(\cdot)}(\mathsf{state}) \end{array}\right] - \frac{1}{2}$$

where SetupO, on input $(x^{(0)} \in \mathcal{X}, x^{(1)} \in \mathcal{X}, M_0 \in \mathcal{M}, M_1 \in \mathcal{M})$, computes $(\mathsf{pk}, \mathsf{msk}) \leftarrow \mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{Y}, \mathcal{M})$, picks $b \leftarrow_{\mathrm{R}} \{0,1\}$, and returns $(\mathsf{pk}, \mathsf{Enc}(\mathsf{pk}, x^{(b)}, M_b)$; $\mathsf{KeyGenO}$, on input y, returns $\mathsf{KeyGen}(\mathsf{msk}, y)$; with the requirement that SetupO is called only once at the beginning of the game, and that all queries y that $\mathcal{A}$ makes to $\mathsf{KeyGenO}(\cdot)$ satisfies $\mathsf{P}(x^{(0)}, y) = \mathsf{P}(x^{(1)}, y)$. Moreover, if $\mathsf{P}(x^{(0)}, y) = 1$, for the queries y to $\mathsf{KeyGenO}$, then $M_0 = M_1$. A PE scheme is *selectively secure*, *fully attribute hiding*, if for all PPT adversaries $\mathcal{A}$, the advantage $\mathsf{Adv}^{\mathsf{PE}}_{\mathcal{A}}(\lambda)$ is a negligible function in λ.

Remark 1 (*Fully vs weakly attribute hiding*)

The fully attribute hiding property refers to the fact that an adversary cannot distinguish a ciphertext for attribute $x^{(0)}$ from a ciphertext for $x^{(1)}$, as long as it only queries keys sk_y where $\mathsf{P}(x^{(0)}, y) = \mathsf{P}(x^{(1)}, y)$. This is stronger that a so-called weakly attribute hiding property, which requires that the adversary only queries keys sk_y where $\mathsf{P}(x^{(0)}, y) = \mathsf{P}(x^{(1)}, y) = 0$.

3 Functional Encryption for Quadratic Functions

In this section we give a functional encryption scheme for quadratic functions, that is, for $n, m \in \mathbb{N}$, $\mathcal{PG} = (p, \mathbb{G}_1, \mathbb{G}_2, P_1, P_2, \mathbb{G}_T, e) \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathcal{X} \subseteq \mathbb{Z}_p^n \times \mathbb{Z}_p^m$, $\mathcal{K} \subseteq \mathbb{Z}_p^{n \times m}$, $\mathcal{Y} \subseteq \mathbb{Z}_p$, and for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}$, $\mathbf{M} \in \mathcal{K}$:

$$F((\mathbf{x}, \mathbf{y}), \mathbf{M}) = \mathbf{x}^\top \mathbf{M} \mathbf{y} \in \mathbb{Z}_p$$

Following the technical overview of Section 1, we first give in Section 3.1 a private-key functional encryption scheme that is only single-ciphertext secure, and we build up from the latter a public-key functional encryption in Section 3.2.

3.1 Private-key, Single-ciphertext secure FE

In Figure 1, we present a family of private-key, single-ciphertext secure functional encryption schemes for quadratic functions, parametrized by an integer $k \geq 1$ and a matrix distribution $\mathcal{D}_k$ (see Definition 1). That is, for each $k \in \mathbb{N}$, and each matrix distribution $\mathcal{D}_k$, the scheme $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$ presented in Figure 1 is single-ciphertext, selectively secure under the $\mathcal{D}_k$-mddh assumption, on asymmetric pairings.

Theorem 1

For any $k \in \mathbb{N}^*$ and any matrix distribution $\mathcal{D}_k$, the functional encryption scheme $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$ defined in Fig. 1 has perfect correctness.

Proof Theorem 1: Correctness follows from the fact that for all $i \in [n], j \in [m]$,

$$e([\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2) = [\mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B} \mathbf{s}_j + (\mathbf{b}^\perp)^\top \mathbf{a}^\perp x_i y_j]_T,$$

since $\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{B}^\top \mathbf{b}^\perp = \mathbf{0}$. Therefore, the decryption computes

$$D := [\sum_{i,j} m_{i,j} \mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B} \mathbf{s}_j + \mathbf{x}^\top \mathbf{M} \mathbf{y} \cdot (\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_T - e(K, [1]_2) - e([1]_1, \widehat{K}) = \mathbf{x}^\top \mathbf{M} \mathbf{y} \cdot [(\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_T.$$

$\underline{\mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{K}, \mathcal{Y}, 1^k, \mathcal{D}_k)}$:
$\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, $\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A})$, $\mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B})$. For $i \in [n], j \in [m]$, $\mathbf{r}_i, \mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$.
Return $\mathsf{pk} := (\mathcal{PG}, [(\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_T)$ and $\mathsf{msk} := \left(\mathbf{A}, \mathbf{a}^\perp, \mathbf{B}, \mathbf{b}^\perp, \{\mathbf{r}_i, \mathbf{s}_j\}_{i\in[n], j\in[m]}\right)$

$\underline{\mathsf{KeyGen}(\mathsf{msk}, \mathbf{M} \in \mathbb{Z}_p^{n\times m})}$:
$u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $K := [\sum_{i\in[n],j\in[m]} m_{i,j} \mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B} \mathbf{s}_j]_1 - [u]_1$, $\widehat{K} := [u]_2$
Return $\mathsf{sk}_{\mathbf{M}} := (K, \widehat{K}) \in \mathbb{G}_1 \times \mathbb{G}_2$

$\underline{\mathsf{Enc}(\mathsf{pk}, \mathsf{msk}, (\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m)}$:
For $i \in [n]$: $\mathbf{c}_i := \mathbf{A}\mathbf{r}_i + \mathbf{b}^\perp x_i$,
For $j \in [m]$: $\widehat{\mathbf{c}}_j := \mathbf{B}\mathbf{s}_j + \mathbf{a}^\perp y_j$,
Return $\mathsf{ct}_{(\mathbf{x},\mathbf{y})} := \{[\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2\}_{i\in[n],j\in[m]} \in \mathbb{G}_1^{n(k+1)} \times \mathbb{G}_2^{m(k+1)}$

$\underline{\mathsf{Dec}(\mathsf{pk}, \mathsf{ct}_{(\mathbf{x},\mathbf{y})}, \mathsf{sk}_{\mathbf{M}})}$:
$D := \sum_{i\in[n],j\in[m]} m_{i,j} \cdot e([\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2) - e(K, [1]_2) - e([1]_1, \widehat{K})$.
Return $v \in \mathbb{Z}_p$ such that $[v \cdot (\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_T = D$.

Figure 1: $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$, a family of private-key, functional encryption schemes parametrized by $k \in \mathbb{N}^*$ and a matrix distribution $\mathcal{D}_k$, single-ciphertext, selectively secure under the $\mathcal{D}_k$-mddh assumption on asymmetric pairings.

Property 1 in Definition 1 implies that $(\mathbf{b}^\perp)^\top \mathbf{a}^\perp \neq 0$ with probability $1 - \frac{1}{\Omega(p)}$ over the choices of $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, and $\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A})$, $\mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B})$. Therefore, one can enumerate all possible $v \in \mathcal{Y}$ and check if $v \cdot [(\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_T = D$. This can be done in time $|\mathcal{Y}|$, thus, we need to set $\mathcal{Y}$ to be of size $\mathsf{poly}(\lambda)$. □

Theorem 2 (*Security*)

For any $k \in \mathbb{N}^*$ and any matrix distribution $\mathcal{D}_k$, if the $\mathcal{D}_k$-mddh assumption holds in $\mathbb{G}_1$ and $\mathbb{G}_2$, then, the private-key functional encryption scheme $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$, defined in Fig. 1, is selectively secure, in a single-ciphertext setting (see the security definition in Section 2.4). Namely, for any PPT adversary $\mathcal{A}$, there exist PPT adversaries $\mathcal{B}$ and $\mathcal{B}'$ such that

$$\mathsf{Adv}^{\mathsf{FE}_{\mathsf{one}}}_{\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathbb{G}_1,\mathcal{B}}(\lambda) + \mathbf{Adv}^{\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathbb{G}_2,\mathcal{B}'}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof Theorem 2: We prove the security of $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$ via a series of games described in Fig. 2 and we use Adv_i to denote the advantage of $\mathcal{A}$ in game G_i.

Lemma 2 ($\mathbf{G_0}$)

$\mathsf{Adv}_0 = \mathsf{Adv}^{\mathsf{FE}_{\mathsf{one}}}_{\mathcal{A}}(\lambda)$.

Proof Lemma 2: We show that G_0 corresponds to the game for selective security of the functional encryption scheme, in the private-key, single-ciphertext setting, as defined in Section 2.4.

$\underline{\mathsf{SetupO}\big((\mathbf{x}^{(0)},\mathbf{y}^{(0)}),(\mathbf{x}^{(1)},\mathbf{y}^{(1)})\big)}$: $\quad \mathrm{G}_0, \boxed{\mathrm{G}_1, \boxed{\mathrm{G}_2}}$

$\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathbf{A},\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, $b \leftarrow_{\mathrm{R}} \{0,1\}$, $\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B})$. For $i \in [n], j \in [m]$: $\mathbf{r}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$

$[\mathbf{c}_i]_1 := [\mathbf{A}\mathbf{r}_i + x_i^{(b)}\mathbf{b}^\perp]_1$; $\boxed{[\mathbf{c}_i]_1 \leftarrow_{\mathrm{R}} \mathbb{G}_1^{k+1}}$

$[\widehat{\mathbf{c}}_j]_2 := [\mathbf{B}\mathbf{s}_j + y_i^{(b)}\mathbf{a}^\perp]_2$; $\boxed{\boxed{[\widehat{\mathbf{c}}_j]_2 \leftarrow_{\mathrm{R}} \mathbb{G}_2^{k+1}}}$

Return $\mathsf{pk} := (\mathcal{PG}, [(\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_T)$ and $\mathsf{ct}_{(\mathbf{x},\mathbf{y})} := \{[\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2\}_{i\in[n],j\in[m]}$

$\underline{\mathsf{KeyGenO}(\mathbf{M} \in \mathbb{Z}_p^{n\times m})}$:

$u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $K := \sum_{i,j} m_{i,j}[\mathbf{c}_i^\top \widehat{\mathbf{c}}_j]_1 - [u]_1 - \mathbf{x}^{(b)\top}\mathbf{M}\mathbf{y}^{(b)} \cdot [(\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_1$, $\widehat{K} := [u]_2$

Return $\mathsf{sk}_{\mathbf{M}} := (K, \widehat{K})$

Figure 2: Games G_0, G_1, G_2 for the proof of selective security of $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$ in Fig. 1. In each procedure, the components inside a solid (dotted) frame are only present in the games marked by a solid (dotted) frame.

It is clear that the oracle SetupO is identically distributed in both of these games. We show that this is also the case of $\mathsf{KeyGenO}$. Indeed, for all $i \in [n]$, $j \in [m]$, we have:

$$\mathbf{c}_i^\top \widehat{\mathbf{c}}_j = \mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_j + x_i^{(b)} y_j^{(b)} (\mathbf{b}^\perp)^\top \mathbf{a}^\perp.$$

Thus, in game G_0, for all $\mathbf{M} \in \mathbb{Z}_p^{n\times m}$, $\mathsf{KeyGenO}(\mathbf{M})$ computes:

$$\begin{aligned} K &:= \sum_{i,j} m_{i,j}[\mathbf{c}_i^\top \widehat{\mathbf{c}}_j]_1 - [u]_1 - \mathbf{x}^{(b)\top}\mathbf{M}\mathbf{y}^{(b)}[(\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_1 \\ &= \sum_{i,j} m_{i,j}[\mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_j]_1 + \mathbf{x}^{(b)\top}\mathbf{M}\mathbf{y}^{(b)}[(\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_1 - [u]_1 - \mathbf{x}^{(b)\top}\mathbf{M}\mathbf{y}^{(b)}[(\mathbf{b}^\perp)^\top \mathbf{a}^\perp]_1 \\ &= \sum_{i,j} m_{i,j}[\mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_j]_1 - [u]_1 \end{aligned}$$

which is exactly as in the security game for selective security. □

Lemma 3 ($\mathbf{G_0}$ *to* $\mathbf{G_1}$)

There exists a PPT adversary $\mathcal{B}_0$ such that

$$|\mathsf{Adv}_0 - \mathsf{Adv}_1| \leq \mathbf{Adv}^{\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathcal{B}_0}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof Lemma 3: Here, we use the mddh assumption on $[\mathbf{A}]_1$ to change the distribution of the challenge ciphertext, after arguing that one can simulate the game without knowing $\mathbf{a}^\perp$ or $[\mathbf{A}]_2$.

Namely, we build a PPT adversary $\mathcal{B}_0'$ against the n-fold mddh assumption in $\mathbb{G}_1$ such that $|\mathsf{Adv}_0 - \mathsf{Adv}_1| \leq \mathbf{Adv}^{n\text{-}\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathbb{G}_1,\mathcal{B}_0'}(\lambda) + 2^{-\Omega(\lambda)}$. Then, by Lemma 1, this implies the existence of a PPT adversary $\mathcal{B}_0$ such that $|\mathsf{Adv}_0 - \mathsf{Adv}_1| \leq \mathbf{Adv}^{\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathbb{G}_1,\mathcal{B}_0}(\lambda) + 2^{-\Omega(\lambda)}$.

Adversary $\mathcal{B}_0'$ simulates the oracles SetupO and $\mathsf{KeyGenO}$ as described in Figure 3. Finally, it outputs 1 if the bit b' output by the adversary $\mathcal{A}$ is equal to b, 0 otherwise. We show that

$\underline{\mathcal{B}'_0\big(\mathcal{PG}, [\mathbf{A}]_1, [\mathbf{h}_1|\cdots|\mathbf{h}_n]_1\big)}$:

Simulation of $\underline{\mathsf{SetupO}\big((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), (\mathbf{x}^{(1)}, \mathbf{y}^{(1)})\big)}$:

$\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, $b \leftarrow_{\mathrm{R}} \{0,1\}$, $\mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B})$, For $j \in [m]$: $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, $\mathbf{z} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$
$\mathbf{c}_i := \mathbf{h}_i + x_i^{(b)}\mathbf{b}^\perp$
$\widehat{\mathbf{c}}_j := \mathbf{B}\mathbf{s}_j + y_j^{(b)}\mathbf{z}$;
Return $\mathsf{pk} := (\mathcal{PG}, [(\mathbf{b}^\perp)^\top \mathbf{z}]_T)$ and $\mathsf{ct} := \{[\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2\}_{i\in[n], j\in[m]}$

Simulation of $\underline{\mathsf{KeyGenO}(\mathbf{M} \in \mathbb{Z}_p^{n\times m})}$:

$u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $K := \sum_{i,j} m_{i,j}[\mathbf{c}_i^\top \widehat{\mathbf{c}}_j]_1 - [u]_1 - \mathbf{x}^{(b)\top}\mathbf{M}\mathbf{y}^{(b)} \cdot [(\mathbf{b}^\perp)^\top \mathbf{z}]_1$, $\widehat{K} := [u]_2$
Return $\mathsf{sk}_{\mathbf{M}} := (K, \widehat{K})$

Figure 3: Adversary $\mathcal{B}'_0$ against the n-fold $\mathcal{D}_k$-mddh assumption, for the proof of Lemma 3.

when $\mathcal{B}'_0$ is given a real mddh challenge, that is, $[\mathbf{h}_1|\cdots|\mathbf{h}_n]_1 := \mathbf{A}\mathbf{R}$ for $\mathbf{R} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k\times n}$, then it simulates the oracles as in game G_0, whereas it simulates them as in game G_1 when given a fully random challenge, i.e. when $[\mathbf{h}_1|\cdots|\mathbf{h}_n]_1 \leftarrow_{\mathrm{R}} \mathbb{G}_1^{(k+1)\times n}$, which implies the lemma.

We use the following facts.

1. For all $\mathbf{s} \in \mathbb{Z}_p^k$, $\mathbf{B} \in \mathbb{Z}_p^{(k+1)\times k}$, $\mathbf{b}^\perp \in \mathsf{orth}(\mathbf{B})$, and $\mathbf{a}^\perp \in \mathbb{Z}_p^{k+1}$, we have:
$$(\mathbf{b}^\perp)^\top \mathbf{a}^\perp = (\mathbf{b}^\perp)^\top (\mathbf{B}\mathbf{s} + \mathbf{a}^\perp).$$

2. For all $y_j^{(b)} \in \mathbb{Z}_p$, $\mathbf{s} \in \mathbb{Z}_p^k$:
$$\big(\{\mathbf{s}_j\}_{j\in[m]}\big)_{\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k} \equiv \Big(\{\mathbf{s}_j + y_j^{(b)}\mathbf{s}\}_{j\in[m]}\Big)_{\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k}.$$

3. $$\Big(\mathbf{B}\mathbf{s} + \mathbf{a}^\perp\Big)_{\mathbf{A},\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k, \mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k} \approx_{\frac{1}{\Omega(p)}} (\mathbf{z})_{\mathbf{z} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}},$$
since $(\mathbf{B}|\mathbf{a}^\perp)$ is a basis of $\mathbb{Z}_p^{k+1}$, with probability $1 - \frac{1}{\Omega(p)}$ over the choices of $\mathbf{A}, \mathbf{B}$, and $\mathbf{a}^\perp$ (this is implied by Property 1).

Therefore, we have for all $\mathbf{y}^{(b)} \in \mathbb{Z}_p^m$:

$$\Big(\mathbf{b}^\perp, \{\mathbf{B}\mathbf{s}_j + y_j^{(b)}\mathbf{a}^\perp\}_{j\in[m]}, (\mathbf{b}^\perp)^\top \mathbf{a}^\perp\Big)_{\mathbf{A},\mathbf{B},\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B}), \mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k}$$
$$\equiv \Big(\mathbf{b}^\perp, \{\mathbf{B}\mathbf{s}_j + y_j^{(b)}\mathbf{a}^\perp\}_{j\in[m]}, (\mathbf{b}^\perp)^\top (\boxed{\mathbf{B}\mathbf{s} + \mathbf{a}^\perp})\Big)_{\mathbf{A},\mathbf{B},\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B}), \boxed{\mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k}, \mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k} \quad \text{(by 1.)}$$
$$\equiv \Big(\mathbf{b}^\perp, \{\mathbf{B}\mathbf{s}_j + y_j^{(b)}(\boxed{\mathbf{B}\mathbf{s} + \mathbf{a}^\perp})\}_{j\in[m]}, (\mathbf{b}^\perp)^\top (\mathbf{B}\mathbf{s} + \mathbf{a}^\perp)\Big)_{\mathbf{A},\mathbf{B},\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B}), \mathbf{s}, \mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k} \quad \text{(by 2.)}$$
$$\approx_{\frac{1}{\Omega(p)}} \Big(\mathbf{b}^\perp, \{\mathbf{B}\mathbf{s}_j + y_j^{(b)}\boxed{\mathbf{z}}\}_{j\in[m]}, (\mathbf{b}^\perp)^\top \boxed{\mathbf{z}}\Big)_{\mathbf{A},\mathbf{B},\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B}), \boxed{\mathbf{z} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}}, \mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k} \quad \text{(by 3.)}$$

Note that the first distribution corresponds to pk, $\{\widehat{\mathbf{c}}_j\}_{j\in[m]}$, and $\mathsf{KeyGenO}$ distributed as in games G_0 or G_1 (these are identically in these two games), while the last distribution corresponds to pk, $\{\widehat{\mathbf{c}}_j\}_{j\in[m]}$, and $\mathsf{KeyGenO}$ simulated by $\mathcal{B}'_0$.

$\mathcal{B}'_0(\mathcal{PG}, [\mathbf{B}]_2, [\mathbf{h}_1|\cdots|\mathbf{h}_m]_2)$:

Simulation of $\mathsf{SetupO}((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), (\mathbf{x}^{(1)}, \mathbf{y}^{(1)}))$:

$\mathbf{A} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, $b \leftarrow_{\mathrm{R}} \{0,1\}$, $\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A})$, $v \leftarrow_{\mathrm{R}} \mathbb{Z}_p$
$\mathbf{c}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$
$\widehat{\mathbf{c}}_j := \mathbf{h}_j + y_j^{(b)}\mathbf{a}^\perp$;
Return $\mathsf{pk} := (\mathcal{PG}, [v]_T)$ and $\mathsf{ct} := \{[\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2\}_{i\in[n],j\in[m]}$

Simulation of $\mathsf{KeyGenO}(\mathbf{M} \in \mathbb{Z}_p^{n\times m})$:

$u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $\widehat{K} := \sum_{i,j} m_{i,j}[\mathbf{c}_i^\top \widehat{\mathbf{c}}_j]_2 - [u]_2 - \mathbf{x}^{(b)\top}\mathbf{M}\mathbf{y}^{(b)} \cdot [v]_1$, $K := [u]_1$
Return $\mathsf{sk}_{\mathbf{M}} := (K, \widehat{K})$

Figure 4: Adversary $\mathcal{B}'_1$ against the m-fold $\mathcal{D}_k$-mddh assumption in $\mathbb{G}_2$, for the proof of Lemma 4.

Finally, when $\mathcal{B}'_0$ is given a real mddh challenge, i.e when for all $i \in [n]$, $\mathbf{h}_i := \mathbf{A}\mathbf{r}_i$, for $\mathbf{r}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, we have $\mathbf{c}_i := \mathbf{A}\mathbf{r}_i + x_i^{(b)}\mathbf{b}^\perp$, exactly as in game G_0, whereas $\mathbf{c}_i$ is uniformly random over $\mathbb{Z}_p^{k+1}$ when $\mathcal{B}'_0$ is given a random challenge, i.e. when for all $i \in [n]$, $\mathbf{h}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$, as in game G_1. □

Lemma 4 ($\mathbf{G_1}$ *to* $\mathbf{G_2}$)

There exists a PPT adversary $\mathcal{B}_1$ such that

$$|\mathsf{Adv}_1 - \mathsf{Adv}_2| \leq \mathbf{Adv}^{\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathbb{G}_2,\mathcal{B}_1}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof Lemma 4: Here, we use the mddh assumption on $[\mathbf{B}]_2$ to change the distribution of the challenge ciphertext, after arguing that one can simulate the game without knowing $\mathbf{b}^\perp$ or $[\mathbf{B}]_1$.

Namely, we build a PPT adversary $\mathcal{B}'_1$ against the m-fold mddh assumption in $\mathbb{G}_2$ such that $|\mathsf{Adv}_1 - \mathsf{Adv}_2| \leq \mathbf{Adv}^{m\text{-}\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathbb{G}_2,\mathcal{B}'_1}(\lambda)$. Then, by Lemma 1, this implies the existence of a PPT adversary $\mathcal{B}_1$ such that $|\mathsf{Adv}_1 - \mathsf{Adv}_2| \leq \mathbf{Adv}^{\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathbb{G}_2,\mathcal{B}_1}(\lambda) + \frac{1}{p-1}$.

Adversary $\mathcal{B}'_1$ simulates the oracles SetupO and $\mathsf{KeyGenO}$ as described in Figure 4. Finally, it outputs 1 if the bit b' output by the adversary $\mathcal{A}$ is equal to b, 0 otherwise. We show that when $\mathcal{B}'_1$ is given a real mddh challenge, that is, $[\mathbf{h}_1|\cdots|\mathbf{h}_m]_2 := [\mathbf{BS}]_2$ for $\mathbf{S} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k\times m}$, then it simulates the oracles as in game G_1, whereas it simulates them as in game G_2 when given a fully random challenge, i.e. when $[\mathbf{h}_1|\cdots|\mathbf{h}_m]_2 \leftarrow_{\mathrm{R}} \mathbb{G}_2^{(k+1)\times m}$, which implies the lemma.

We use the fact that for all $\mathbf{A}, \mathbf{B} \in \mathbb{Z}_p^{(k+1)\times k}$,

$$(\mathbf{a}^\perp, (\mathbf{b}^\perp)^\top \mathbf{a}^\perp)_{\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B})} \equiv (\mathbf{a}^\perp, v)_{v \leftarrow_{\mathrm{R}} \mathbb{Z}_p)}.$$

Note that the leftmost distribution corresponds to pk, $\{\mathbf{c}_i\}_{i\in[n]}$, and $\mathsf{KeyGenO}$ distributed as in games G_1 or G_2 (these are identically distributed in these two games), while the last distribution corresponds to pk, $\{\mathbf{c}_i\}_{i\in[n]}$, and $\mathsf{KeyGenO}$ simulated by $\mathcal{B}'_1$.

Finally, when $\mathcal{B}'_1$ is given a real mddh challenge, i.e when for all $j \in [m]$, $\mathbf{h}_j := \mathbf{B}\mathbf{s}_j$, for $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, we have $\widehat{\mathbf{c}}_j := \mathbf{B}\mathbf{s}_j + y_j^{(b)}\mathbf{a}^\perp$, exactly as in game G_1, whereas $\widehat{\mathbf{c}}_j$ is uniformly random over $\mathbb{Z}_p^{k+1}$ when $\mathcal{B}'_1$ is given a random challenge, i.e. when for all $j \in [m]$, $\mathbf{h}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$, as in game G_2. □

Lemma 5 (G_2)

$\mathsf{Adv}_2 = 0$.

Proof Lemma 5: By definition of the security game, for all $\mathbf{M}$ queried to $\mathsf{KeyGen0}$, we have: $\mathbf{x}^{(b)\top}\mathbf{M}\mathbf{y}^{(b)} = \mathbf{x}^{(0)\top}\mathbf{M}\mathbf{y}^{(0)}$. Therefore, the view of the adversary in G_2 is completely independent from the random bit $b \leftarrow_R \{0,1\}$. □

Combining Lemma 3, 4, and 5 gives Theorem 2. □

3.2 Public-key FE

In Figure 3, we present a family of public-key functional encryption schemes for quadratic functions, parametrized by an integer $k \geq 1$ and a matrix distribution $\mathcal{D}_k$ (see Definition 1). That is, for each $k \in \mathbb{N}$, and each matrix distribution $\mathcal{D}_k$, the scheme $\mathsf{FE}(k, \mathcal{D}_k)$ presented in Figure 5 is selectively secure under the $\mathcal{D}_k$-mddh and the 3-pddh assumptions, on asymmetric pairings.

$\underline{\mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{K}, \mathcal{Y}, 1^k, \mathcal{D}_k)}$:
$\mathcal{PG} \leftarrow_R \mathsf{GGen}(1^\lambda)$, $\mathbf{A}, \mathbf{B} \leftarrow_R \mathcal{D}_k$;
For $i \in [2n], j \in [2m]$, $\mathbf{r}_i, \mathbf{s}_j \leftarrow_R \mathbb{Z}_p^k$.
Return $\mathsf{pk} := \{[\mathbf{r}_i^\top \mathbf{A}^\top]_1, [\mathbf{B}\mathbf{s}_j]_2\}_{i\in[2n],j\in[2m]}$ and $\mathsf{msk} := \left(\mathbf{A}, \mathbf{B}, \{\mathbf{r}_i, \mathbf{s}_j\}_{i\in[2n],j\in[2m]}\right)$

$\underline{\mathsf{KeyGen}(\mathsf{msk}, \mathbf{M} \in \mathbb{Z}_p^{n\times m})}$:
$u \leftarrow_R \mathbb{Z}_p$, $K := [\sum_{i\in[n],j\in[m]} m_{i,j}\left(\mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_j + \mathbf{r}_{n+i}^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_{m+j}\right)]_1 - [u]_1 \in \mathbb{G}_1$, $\widehat{K} := [u]_2 \in \mathbb{G}_2$.
Return $\mathsf{sk}_\mathbf{M} := (K, \widehat{K}) \in \mathbb{G}_1 \times \mathbb{G}_2$

$\underline{\mathsf{Enc}(\mathsf{pk}, (\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m)}$:
$\mathbf{V}, \mathbf{W} \leftarrow_R \mathsf{GL}_{k+2}$, $\gamma \leftarrow_R \mathbb{Z}_p$, $c_0 = \widehat{c}_0 := \gamma$, for all $i \in [n], j \in [m]$:
$\mathbf{c}_i := \begin{pmatrix} \gamma \cdot \mathbf{A}\mathbf{r}_i \\ x_i \end{pmatrix}^\top \mathbf{W}^{-1}$, $\mathbf{c}_{n+i} := \begin{pmatrix} \gamma \cdot \mathbf{A}\mathbf{r}_{n+i} \\ 0 \end{pmatrix}^\top \mathbf{V}^{-1}$,
$\widehat{\mathbf{c}}_j := \mathbf{W}\begin{pmatrix} \mathbf{B}\mathbf{s}_j \\ y_j \end{pmatrix}$, $\widehat{\mathbf{c}}_{m+j} := \mathbf{V}\begin{pmatrix} \mathbf{B}\mathbf{s}_{m+j} \\ 0 \end{pmatrix}$
$\mathsf{ct}_{(\mathbf{x},\mathbf{y})} := \{[c_0]_1, [\widehat{c}_0]_2, [\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2\}_{i\in[2n],j\in[2m]} \in \mathrm{G}_1^{2n(k+2)+1} \times \mathrm{G}_2^{2m(k+2)+1}$

$\underline{\mathsf{Dec}(\mathsf{mpk}, \mathsf{ct}_{(\mathbf{x},\mathbf{y})}, \mathsf{sk}_\mathbf{F})}$:
Return $\sum_{i\in[n],j\in[m]} m_{i,j}\left(e([\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2) + e([\mathbf{c}_{n+i}]_1, [\widehat{\mathbf{c}}_{m+j}]_2)\right) - e([c_0]_1, \widehat{K}) - e(K, [\widehat{c}_0]_2)$.

Figure 5: $\mathsf{FE}(k, \mathcal{D}_k)$, a family of functional encryption schemes parametrized by $k \in \mathbb{N}^*$ and a matrix distribution $\mathcal{D}_k$, selectively secure under the $\mathcal{D}_k$-mddh and 3-pddh assumptions.

Theorem 3 (*Correctness*)

For any $k \in \mathbb{N}^*$ and any matrix distribution $\mathcal{D}_k$, the functional encryption scheme $\mathsf{FE}(k, \mathcal{D}_k)$ defined in Figure 5 has perfect correctness.

Proof Theorem 3: Correctness follows from the facts that for all $i \in [n]$, $j \in [m]$:

$$e([\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2) = [\gamma \mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_j + x_i y_j]_T \text{ and } e([\mathbf{c}_{n+i}]_1, [\widehat{\mathbf{c}}_{m+j}]_2) = [\gamma \mathbf{r}_{n+i}^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_{m+j}]_T.$$

$\underline{\mathsf{SetupO}\big((\mathbf{x}^{(0)},\mathbf{y}^{(0)}),(\mathbf{x}^{(1)},\mathbf{y}^{(1)})\big)}$: $\mathrm{G}_0, \boxed{\mathrm{G}_1, \boxed{\mathrm{G}_2, \mathrm{G}_3}, \mathrm{G}_4}, \mathrm{G}_5$

$\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$; $\mathbf{A},\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$; $b \leftarrow_{\mathrm{R}} \{0,1\}$; $\boxed{\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B})}$

For $i \in [2n], j \in [2m]$: $\mathbf{r}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$

$$\mathsf{pk} := \left\{ \left[\mathbf{A}\mathbf{r}_i + \boxed{x_i^{(b)}\mathbf{b}^\perp}\right]_1, \left[\mathbf{A}\mathbf{r}_{n+i} - \boxed{x_i^{(0)}\mathbf{b}^\perp}\right]_1, \left[\mathbf{B}\mathbf{s}_j + \boxed{y_j^{(b)}\mathbf{a}^\perp}\right]_2, \left[\mathbf{B}\mathbf{s}_{m+j} + \boxed{y_j^{(0)}\mathbf{a}^\perp}\right]_2 \right\}_{i\in[n],j\in[m]},$$

$\mathbf{V},\mathbf{W} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$, $\gamma \leftarrow_{\mathrm{R}} \mathbb{Z}_p$; $\boxed{v \leftarrow_{\mathrm{R}} \mathbb{Z}_p}$; $c_0 = \widehat{c}_0 := \gamma$

$$\mathbf{c}_i := \begin{pmatrix} \gamma\cdot\mathbf{A}\mathbf{r}_i + \boxed{\gamma x_i^{(b)}\mathbf{b}^\perp} + \boxed{v x_i^{(b)}\mathbf{b}^\perp} \\ x_i^{(b)} - \boxed{x_i^{(b)}} \end{pmatrix}^\top \mathbf{W}^{-1},\ \mathbf{c}_{n+i} := \begin{pmatrix} \gamma\cdot\mathbf{A}\mathbf{r}_{n+i} - \boxed{\gamma x_i^{(0)}\mathbf{b}^\perp} - \boxed{v x_i^{(0)}\mathbf{b}^\perp} \\ 0 + \boxed{x_i^{(0)}} \end{pmatrix}^\top \mathbf{V}^{-1},$$

$$\widehat{\mathbf{c}}_j := \mathbf{W}\begin{pmatrix} \mathbf{B}\mathbf{s}_j + \boxed{y_j^{(b)}\mathbf{a}^\perp} \\ y_j - \boxed{y_j^{(b)}} \end{pmatrix},\ \widehat{\mathbf{c}}_{m+j} := \mathbf{V}\begin{pmatrix} \mathbf{B}\mathbf{s}_{m+j} + \boxed{y_j^{(0)}\mathbf{a}^\perp} \\ 0 + \boxed{y_j^{(0)}} \end{pmatrix}$$

Return pk and $\mathsf{ct}_{(\mathbf{x},\mathbf{y})} := \{[\mathbf{c}_i]_1, [\widehat{\mathbf{c}}_j]_2\}_{i\in[2n],j\in[2m]}$

$\underline{\mathsf{KeyGenO}(\mathbf{M} \in \mathbb{Z}_p^{n\times m})}$:

$u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $K := [\sum_{i\in[n],j\in[m]} m_{i,j}\big(\mathbf{r}_i^\top\mathbf{A}^\top\mathbf{B}\mathbf{s}_j + \mathbf{r}_{n+i}^\top\mathbf{A}^\top\mathbf{B}\mathbf{s}_{m+j}\big)]_1 - [u]_1 \in \mathbb{G}_1$; $\widehat{K} := [u]_2 \in \mathbb{G}_2$.

Return $\mathsf{sk}_{\mathbf{M}} := (K, \widehat{K}) \in \mathbb{G}_1 \times \mathbb{G}_2$

Figure 6: Games G_i, $i = 0,\ldots,5$ for the proof of selective security of $\mathsf{FE}(k,\mathcal{D}_k)$ in Fig. 5. In each procedure, the components inside a solid (dotted, gray) frame are only present in the games marked by a solid (dotted, gray) frame.

Therefore, the decryption gets

$$\begin{aligned}
&[\sum_{i\in[n],j\in[m]} m_{i,j}\gamma\big(\mathbf{r}_i^\top\mathbf{A}^\top\mathbf{B}\mathbf{s}_j + \mathbf{r}_{n+i}^\top\mathbf{A}^\top\mathbf{B}\mathbf{s}_{m+j}\big)]_T \\
&+ [\sum_{i\in[n],j\in[m]} m_{i,j}x_iy_j]_T - e([c_0]_1, \widehat{K}) - e(K, [\widehat{c}_0]_2) \\
&= [\sum_{i\in[n],j\in[m]} m_{i,j}x_iy_j]_T.
\end{aligned}$$

Then, the decryption solves the discrete log to recover $\mathbf{x}^\top\mathbf{M}\mathbf{y} \in \mathbb{Z}_p$, which can be done efficiently as long as the set $\mathcal{Y}$ is of size $\mathsf{poly}(\lambda)$. □

Theorem 4 (*Security*)

For any $k \in \mathbb{N}^*$ and any matrix distribution $\mathcal{D}_k$, if the $\mathcal{D}_k$-mddh and the 3-pddh assumptions hold in $\mathcal{PG}$, then the functional encryption scheme $\mathsf{FE}(k,\mathcal{D}_k)$ defined in Figure 5 is selectively secure. Namely, for any PPT adversary $\mathcal{A}$, there exists PPT adversaries $\mathcal{B}$, $\mathcal{B}'$ and $\mathcal{B}''$ such that

$$\mathsf{Adv}^{\mathsf{FE}}_{\mathcal{A}}(\lambda) \le 4\cdot\mathbf{Adv}^{\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_1,\mathcal{B}}(\lambda) + 4\cdot\mathbf{Adv}^{\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_2,\mathcal{B}'}(\lambda) + 2\cdot\mathbf{Adv}^{3-\mathsf{pddh}}_{\mathsf{GGen},\mathcal{B}'}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof Theorem 4: We prove the security of $\mathsf{FE}(k,\mathcal{D}_k)$ via a series of games described in Figure 3.2 and we use Adv_i to denote the advantage of $\mathcal{A}$ in game G_i. G_0 corresponds to the

game for selective security of the functional encryption scheme, as defined in Section 2.4.2

Lemma 6 ($\mathbf{G_0}$ *to* $\mathbf{G_1}$)

There exists PPT adversaries $\mathcal{B}_0$ and $\mathcal{B}_1$ such that

$$|\mathsf{Adv}_0 - \mathsf{Adv}_1| \leq 2 \cdot \mathbf{Adv}^{\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_1,\mathcal{B}_0}(\lambda) + 2 \cdot \mathbf{Adv}^{\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_2,\mathcal{B}_1}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof Lemma 6: Using the selective, single-ciphertext security of the underlying private-key scheme (which is exactly the scheme in Figure 1), we can change the distribution of the public key elements from $\{[\mathbf{A}\mathbf{r}_i]_1, [\mathbf{B}\mathbf{s}_j]_2\}_{i\in[2n],j\in[2m]}$ to

$$\left\{[\mathbf{A}\mathbf{r}_i + rx_i^{(b)}\mathbf{b}^\perp]_1, [\mathbf{A}\mathbf{r}_{n+i} - rx_i^{(0)}\mathbf{b}^\perp]_1, [\mathbf{B}\mathbf{s}_j + sy_j^{(b)}\mathbf{a}^\perp]_2, [\mathbf{B}\mathbf{s}_{m+j} + sy_j^{(0)}\mathbf{a}^\perp]_2\right\}_{i\in[n],j\in[m]}.$$

In order to apply Theorem 2 we rely on the fact that the FE public key can be seen as an $\mathsf{FE}_{\mathsf{one}}$ encryption of longer vectors

$$\widetilde{\mathbf{x}}^{(0)} = \mathbf{0} \in \mathbb{Z}_p^{2n} \text{ and } \widetilde{\mathbf{y}}^{(0)} = \mathbf{0} \in \mathbb{Z}_p^{2m} \text{ in } G_0,$$

$$\widetilde{\mathbf{x}}^{(1)} = (\mathbf{x}^{(b)}||-\mathbf{x}^{(0)}) \in \mathbb{Z}_p^{2n} \text{ and } \widetilde{\mathbf{y}}^{(1)} = (\mathbf{y}^{(b)}||\mathbf{y}^{(0)}) \in \mathbb{Z}_p^{2m} \text{ in } G_1.$$

Also, secret keys in FE can be seen as $\mathsf{FE}_{\mathsf{one}}$ secret keys corresponding to matrices

$$\widetilde{\mathbf{M}} = \left(\begin{array}{c|c} \mathbf{M} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{M} \end{array}\right) \in \mathbb{Z}_p^{2n\times 2m}$$

With this observation in mind, it can be seen that the restriction

$$\mathbf{x}^{(1)\top}\mathbf{M}\,\mathbf{y}^{(1)} = \mathbf{x}^{(0)\top}\mathbf{M}\,\mathbf{y}^{(0)}$$

in the queries made by $\mathcal{A}$ translates into legitimate queries by $\mathcal{B}_0$ since $\mathbf{x}^{(b)\top}\mathbf{M}\,\mathbf{y}^{(b)} - \mathbf{x}^{(0)\top}\mathbf{M}\,\mathbf{y}^{(0)} = 0$ and $\widetilde{\mathbf{x}}^{(0)\top}\widetilde{\mathbf{M}}\,\widetilde{\mathbf{y}}^{(0)} = \widetilde{\mathbf{x}}^{(1)\top}\widetilde{\mathbf{M}}\,\widetilde{\mathbf{y}}^{(1)} = 0$. Thus, by Theorem 2 (security of the single-ciphertext secure scheme), we obtain the lemma. □

Lemma 7 ($\mathbf{G_1}$ *to* $\mathbf{G_2}$)

There exists a PPT adversary $\mathcal{B}_2$

$$|\mathsf{Adv}_1 - \mathsf{Adv}_2| \leq \mathbf{Adv}^{3-\mathsf{pddh}}_{\mathsf{GGen},\mathcal{B}_2}(\lambda) + 2^{-\Omega(\lambda)}$$

Here, we change the distribution of the challenge ciphertexts, using the 3-pddh assumption.

Proof Lemma 7: Upon receiving a 3-pddh challenge $(\mathcal{PG}, [a]_1, [b]_2, [c]_1, [c]_2, [z]_1)$ (see Definition 3), $\mathcal{B}_2$ simulates $\mathsf{SetupO}(\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), (\mathbf{x}^{(1)}, \mathbf{y}^{(1)}$ by picking $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$; $b \leftarrow_{\mathrm{R}} \{0,1\}$; $\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B})$, and setting$[\gamma]_1 := [c]_1$ and $[\gamma]_2 := [c]_2$. Then, for $i \in [2n], j \in [2m]$, $\mathcal{B}_2$ picks $\mathbf{r}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and computes

$$\mathsf{pk} := \left\{\left[\mathbf{A}\mathbf{r}_i + ax_i^{(b)}\mathbf{b}^\perp\right]_1, \left[\mathbf{A}\mathbf{r}_{n+i} - ax_i^{(0)}\mathbf{b}^\perp\right]_1, \left[\mathbf{B}\mathbf{s}_j + by_j^{(b)}\mathbf{a}^\perp\right]_2, \left[\mathbf{B}\mathbf{s}_{m+j} + by_j^{(0)}\mathbf{a}^\perp\right]_2\right\}_{i\in[n],j\in[m]}.$$

It picks $\widetilde{\mathbf{W}}, \widetilde{\mathbf{V}} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$ and implicitly sets

$$\mathbf{W} := \widetilde{\mathbf{W}}\left(\begin{array}{c|c} \mathbf{B}|b\cdot\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1} \text{ and } \mathbf{V} := \widetilde{\mathbf{V}}\left(\begin{array}{c|c} \mathbf{B}|b\cdot\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1}.$$

Here we use the fact that $(\mathbf{B}|b\mathbf{a}^\perp)$ is full rank with probability $1-\frac{1}{\Omega(p)}$ over $\mathbf{A},\mathbf{B}\leftarrow_{\mathrm{R}}\mathcal{D}_k$, $\mathbf{a}^\perp\mathsf{orth}(\mathbf{A})$, and $b\leftarrow_{\mathrm{R}}\mathbb{Z}_p$ (this is implied by Property 1).

Then, for $i\in[n], j\in[m]$, it computes

$$[\mathbf{c}_i]_1 := \left[\begin{pmatrix}\gamma\mathbf{r}_i\\ z\cdot x_i^{(b)}\\ x_i^{(b)}\end{pmatrix}^\top \left(\begin{array}{c|c|c}\mathbf{A}^\top\mathbf{B} & 0 & 0\\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 0\\ \hline 0 & 0 & 1\end{array}\right)\widetilde{\mathbf{W}}^{-1}\right]_1 \text{ and } [\widehat{\mathbf{c}}_j]_2 := \left[\widetilde{\mathbf{W}}\begin{pmatrix}\mathbf{s}_j\\ y_j^{(b)}\\ y_j^{(b)}\end{pmatrix}\right]_2$$

$$[\mathbf{c}_{n+i}]_1 := \left[\begin{pmatrix}\gamma\mathbf{r}_{n+i}\\ -z\cdot x_i^{(0)}\\ 0\end{pmatrix}^\top \left(\begin{array}{c|c|c}\mathbf{A}^\top\mathbf{B} & 0 & 0\\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 0\\ \hline 0 & 0 & 1\end{array}\right)\widetilde{\mathbf{V}}^{-1}\right]_1 \text{ and } [\widehat{\mathbf{c}}_{m+j}]_2 := \left[\widetilde{\mathbf{V}}\begin{pmatrix}\mathbf{s}_{m+j}\\ y_j^{(0)}\\ 0\end{pmatrix}\right]_2.$$

$\mathcal{B}_2$ computes $[c_0]_1 := [\gamma]_1$, $[\widehat{c}_0]_2 := [\gamma]_2$, and simulates $\mathsf{KeyGen0}$ as in G_2 (see Figure 3.2). Finally, if $\mathcal{A}$ outputs b', $\mathcal{B}_2$ outputs 1 if $b'=b$, and 0 otherwise.

It can be seen that when $[z]_1$ is a real 3-pddh challenge, i.e., $[z]_1=[abc]_1$, then $\mathcal{B}_2$ simulates game G_1; whereas it simulates game G_2 when $[z]_1\leftarrow_{\mathrm{R}}\mathbb{G}_1$. In particular, while this is easy to see for the elements of the public key and for ciphertexts $[\widehat{\mathbf{c}}_j]_2$, $[\widehat{\mathbf{c}}_{m+j}]_2$, for the ciphertext elements $[\mathbf{c}_i]_1$, $[\mathbf{c}_{n+i}]_1$ we observe that they can be written as

$$\mathbf{c}_i := \begin{pmatrix}\gamma\mathbf{B}^\top\mathbf{A}\mathbf{r}_i\\ z\cdot x_i^{(b)}\cdot(\mathbf{b}^\perp)^\top\mathbf{a}^\perp\\ x_i^{(b)}\end{pmatrix}^\top \left(\begin{array}{c|c}\mathbf{B}|b\cdot\mathbf{a}^\perp & 0\\ \hline \mathbf{0} & 1\end{array}\right)^{-1}\mathbf{W}^{-1} = \begin{pmatrix}\gamma\mathbf{A}\mathbf{r}_i + zb^{-1}\cdot x_i^{(b)}\\ x_i^{(b)}\end{pmatrix}^\top\mathbf{W}^{-1}$$

$$\mathbf{c}_{n+i} := \begin{pmatrix}\gamma\mathbf{B}^\top\mathbf{A}\mathbf{r}_{n+i}\\ -z\cdot x_i^{(0)}\cdot(\mathbf{b}^\perp)^\top\mathbf{a}^\perp\\ 0\end{pmatrix}^\top \left(\begin{array}{c|c}\mathbf{B}|b\cdot\mathbf{a}^\perp & 0\\ \hline \mathbf{0} & 1\end{array}\right)^{-1}\mathbf{V}^{-1} = \begin{pmatrix}\gamma\mathbf{A}\mathbf{r}_{n+i} + zb^{-1}\cdot x_i^{(0)}\\ 0\end{pmatrix}^\top\mathbf{V}^{-1}.$$

So, if $z=abc$, then $zb^{-1}=a\gamma$ and the ciphertexts are distributed as in G_1; otherwise if z is random zb^{-1} is identically distributed to $(a\gamma+v)$ as in G_2. This proves $|\mathsf{Adv}_1-\mathsf{Adv}_2|\le \mathbf{Adv}^{3-\mathsf{pddh}}_{\mathsf{GGen},\mathcal{B}_2}(\lambda)+2^{-\Omega(\lambda)}$. □

Lemma 8 (G_2 *to* G_3)

$|\mathsf{Adv}_2-\mathsf{Adv}_3|\le 2^{-\Omega(\lambda)}$.

Here, we change the distribution of the challenge ciphertexts, using a statistical argument.

Proof Lemma 8: First, we use the fact that for all $\gamma\in\mathbb{Z}_p$:

$$(\gamma, v+\gamma)_{v\leftarrow_{\mathrm{R}}\mathbb{Z}_p} \equiv (\gamma, v)_{v\leftarrow_{\mathrm{R}}\mathbb{Z}_p}.$$

Therefore, we can write the challenge ciphertexts as follows. For all i$\in[n], j\in[m]$:

$$\mathbf{c}_i := \begin{pmatrix}\gamma\mathbf{A}\mathbf{r}_i + vx_i^{(b)}\mathbf{b}^\perp\\ x_i^{(b)}\end{pmatrix}^\top\mathbf{W}^{-1}, \mathbf{c}_{n+i} := \begin{pmatrix}\gamma\mathbf{A}\mathbf{r}_{n+i} - vx_i^{(0)}\mathbf{b}^\perp\\ 0\end{pmatrix}^\top\mathbf{V}^{-1}.$$

Then, we use the facts that:

- $(v\leftarrow_{\mathrm{R}}\mathbb{Z}_p)\approx_{\frac{1}{p}}(v\leftarrow_{\mathrm{R}}\mathbb{Z}_p)$ such that $v+1\neq 0 \mod p$.
- $(\mathbf{A},\mathbf{B},\mathbf{a}^\perp)_{\mathbf{A},\mathbf{B}\leftarrow_{\mathrm{R}}\mathcal{D}_k,\mathbf{a}^\perp\leftarrow_{\mathrm{R}}\mathsf{orth}(\mathbf{A})}\approx_{\frac{1}{\Omega(p)}}(\mathbf{A},\mathbf{B},\mathbf{a}^\perp)_{\mathbf{A},\mathbf{B}\leftarrow_{\mathrm{R}}\mathcal{D}_k,\mathbf{a}^\perp\leftarrow_{\mathrm{R}}\mathsf{orth}(\mathbf{A})\setminus\mathsf{span}(\mathbf{B})}$, by Property 1.

- For any $v \in \mathbb{Z}_p$ such that $v+1 \neq 0 \mod p$, $\mathbf{W} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$ is identically distributed than $\widetilde{\mathbf{W}} \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & \frac{v}{v+1} & \frac{1}{v+1} \\ \hline 0 & -1 & 1 \end{array}\right) \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1}$, where $\widetilde{\mathbf{W}} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$, $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, and $\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}) \setminus \mathsf{span}(\mathbf{B})$.

Therefore, we can change the distribution of $\{\mathbf{c}_i, \widehat{\mathbf{c}}_j\}_{i\in[n],j\in[m]}$ as follows:

$$\begin{aligned}
\widehat{\mathbf{c}}_j &= \widetilde{\mathbf{W}} \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & \frac{v}{v+1} & \frac{1}{v+1} \\ \hline 0 & -1 & 1 \end{array}\right) \begin{pmatrix} \mathbf{s}_j \\ y_j^{(b)} \\ y_j^{(b)} \end{pmatrix} \\
&= \widetilde{\mathbf{W}} \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right) \cdot \begin{pmatrix} \mathbf{s}_j \\ y_j^{(b)} \\ 0 \end{pmatrix} \\
&= \widetilde{\mathbf{W}} \cdot \begin{pmatrix} \mathbf{B}\mathbf{s}_j + y_j^{(b)}\mathbf{a}^\perp \\ 0 \end{pmatrix}
\end{aligned}$$

and

$$\begin{aligned}
\mathbf{c}_i &= \begin{pmatrix} \gamma\mathbf{r}_i \\ v x_i^{(b)} \\ x_i^{(b)} \end{pmatrix}^\top \left(\begin{array}{c|c|c} \mathbf{A}^\top\mathbf{B} & 0 & 0 \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & \frac{v}{v+1} & \frac{1}{v+1} \\ \hline 0 & -1 & 1 \end{array}\right)^{-1} \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1} \cdot \widetilde{\mathbf{W}}^{-1} \\
&= \begin{pmatrix} \gamma\mathbf{r}_i \\ v \cdot x_i^{(b)} \\ x_i^{(b)} \end{pmatrix}^\top \left(\begin{array}{c|c|c} \mathbf{A}^\top\mathbf{B} & 0 & 0 \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & \frac{-1}{v+1} \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & \frac{v}{v+1} \end{array}\right) \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1} \cdot \widetilde{\mathbf{W}}^{-1} \\
&= \begin{pmatrix} \gamma\mathbf{r}_i \\ (v+1) \cdot x_i^{(b)} \\ 0 \end{pmatrix}^\top \cdot \left(\begin{array}{c|c|c} \mathbf{A}^\top\mathbf{B} & 0 & 0 \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1} \cdot \widetilde{\mathbf{W}}^{-1} \\
&= \begin{pmatrix} \gamma\mathbf{A}\mathbf{r}_i + (v+1) \cdot x_i^{(b)}\mathbf{b}^\perp \\ 0 \end{pmatrix}^\top \cdot \widetilde{\mathbf{W}}^{-1}
\end{aligned}$$

Then, we use the facts that:

- $v \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ such that $v+1 \neq 0 \mod p \approx_{\frac{1}{p}} v \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ such that $v+1 \neq 0 \mod p$ and $v \neq 0 \mod p$.
- For any $v \in \mathbb{Z}_p$ such that $v+1 \neq 0 \mod p$ and $v \neq 0 \mod p$, $\mathbf{V} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$ is identically distributed than $\widetilde{\mathbf{V}} \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & 1 & \frac{1}{v} \\ \hline 0 & 1 & 1+\frac{1}{v} \end{array}\right) \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1}$, where $\widetilde{\mathbf{V}} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$, $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, and $\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}) \setminus \mathsf{span}(\mathbf{B})$.

Therefore, we can change the distribution of $\{\mathbf{c}_{n+i}, \widehat{\mathbf{c}}_{m+j}\}_{i\in[n],j\in[m]}$ as follows:

$$\begin{aligned}
\widehat{\mathbf{c}}_{m+j} &= \widetilde{\mathbf{V}} \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & 1 & \frac{1}{v} \\ \hline 0 & 1 & 1+\frac{1}{v} \end{array}\right) \begin{pmatrix} \mathbf{s}_j \\ y_j^{(0)} \\ 0 \end{pmatrix} \\
&= \widetilde{\mathbf{V}} \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right) \cdot \begin{pmatrix} \mathbf{s}_j \\ y_j^{(0)} \\ y_j^{(0)} \end{pmatrix} \\
&= \widetilde{\mathbf{V}} \cdot \begin{pmatrix} \mathbf{B}\mathbf{s}_j + y_j^{(0)}\mathbf{a}^\perp \\ y_j^{(0)} \end{pmatrix}
\end{aligned}$$

and

$$\begin{aligned}
\mathbf{c}_{n+i} &= \begin{pmatrix} \gamma\mathbf{r}_{n+i} \\ -vx_i^{(0)} \\ 0 \end{pmatrix}^\top \left(\begin{array}{c|c|c} \mathbf{A}^\top\mathbf{B} & 0 & 0 \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & 1 & \frac{1}{v} \\ \hline 0 & 1 & 1+\frac{1}{v} \end{array}\right)^{-1} \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1} \cdot \widetilde{\mathbf{V}}^{-1} \\
&= \begin{pmatrix} \gamma\mathbf{r}_{n+i} \\ -vx_i^{(0)} \\ 0 \end{pmatrix}^\top \left(\begin{array}{c|c|c} \mathbf{A}^\top\mathbf{B} & 0 & 0 \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp \cdot (1+\frac{1}{v}) & \frac{-1}{v} \\ \hline 0 & -(\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 1 \end{array}\right) \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1} \cdot \widetilde{\mathbf{V}}^{-1} \\
&= \begin{pmatrix} \gamma\mathbf{r}_{n+i} \\ -(v+1)x_i^{(0)} \\ x_i^{(0)} \end{pmatrix}^\top \left(\begin{array}{c|c|c} \mathbf{A}^\top\mathbf{B} & 0 & 0 \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1} \cdot \widetilde{\mathbf{V}}^{-1} \\
&= \begin{pmatrix} \gamma\mathbf{A}\mathbf{r}_{n+i} - (v+1)x_i^{(0)}\mathbf{b}^\perp \\ x_i^{(0)} \end{pmatrix}^\top \cdot \widetilde{\mathbf{V}}^{-1}
\end{aligned}$$

Finally, we use the fact that for any $\gamma \in \mathbb{Z}_p$: $(v+1)$ where $v \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ such that $v+1 \neq 0 \mod p$ and $v \neq 0 \mod p \approx_{\frac{2}{p}} (v+\gamma)$, where $v \leftarrow_{\mathrm{R}} \mathbb{Z}_p$. Thus, we obtain, for all $i \in [n]$ and $j \in [m]$:

$$\mathbf{c}_i := \begin{pmatrix} \gamma\mathbf{A}\mathbf{r}_i + (v+\gamma)x_i^{(b)}\mathbf{b}^\perp \\ 0 \end{pmatrix}^\top \widetilde{\mathbf{W}}^{-1}, \mathbf{c}_{n+i} := \begin{pmatrix} \gamma\mathbf{A}\mathbf{r}_{n+i} - (v+\gamma)x_i^{(0)}\mathbf{b}^\perp \\ x_i^{(0)} \end{pmatrix}^\top \widetilde{\mathbf{V}}^{-1},$$

$\widehat{\mathbf{c}}_j := \widetilde{\mathbf{W}} \begin{pmatrix} \gamma\mathbf{B}\mathbf{s}_j + y_j^{(b)}\mathbf{a}^\perp \\ 0 \end{pmatrix}$, $\widehat{\mathbf{c}}_{m+j} := \widetilde{\mathbf{V}} \begin{pmatrix} \gamma\mathbf{B}\mathbf{s}_j + y_j^{(0)}\mathbf{a}^\perp \\ y_j^{(0)} \end{pmatrix}$, as in game G_3.

This proves $|\mathsf{Adv}_2 - \mathsf{Adv}_3| \leq 2^{-\Omega(\lambda)}$. □

Lemma 9 ($\mathbf{G_3}$ *to* $\mathbf{G_4}$)

There exists an adversary $\mathcal{B}_3$ such that

$$|\mathsf{Adv}_3 - \mathsf{Adv}_4| \leq \mathbf{Adv}^{3-\mathsf{pddh}}_{\mathsf{GGen},\mathcal{B}_3}(\lambda) + 2^{-\Omega(\lambda)}.$$

Here, we change the distribution of the challenge ciphertext, using the 3-pddh assumption, as for Lemma 7.

Proof Lemma 9: Upon receiving a 3-pddh challenge $(\mathcal{PG}, [a]_1, [b]_2, [c]_1, [c]_2, [z]_1)$ (see Definition 3), $\mathcal{B}_3$ simulates $\mathsf{SetupO}((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), (\mathbf{x}^{(1)}, \mathbf{y}^{(1)}))$ by picking $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$; $b \leftarrow_{\mathrm{R}} \{0,1\}$; $\mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{A}), \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathsf{orth}(\mathbf{B})$, and setting: $[\gamma]_1 := [c]_1$ and $[\gamma]_2 := [c]_2$. Then, for $i \in [2n], j \in [2m]$, $\mathcal{B}_3$ picks $\mathbf{r}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and computes

$$\mathsf{pk} := \left\{ \left[\mathbf{A}\mathbf{r}_i + a x_i^{(b)} \mathbf{b}^\perp\right]_1, \left[\mathbf{A}\mathbf{r}_{n+i} - a x_i^{(0)} \mathbf{b}^\perp\right]_1, \left[\mathbf{B}\mathbf{s}_j + b y_j^{(b)} \mathbf{a}^\perp\right]_2, \left[\mathbf{B}\mathbf{s}_{m+j} + b y_j^{(0)} \mathbf{a}^\perp\right]_2 \right\}_{i\in[n], j\in[m]}.$$

It picks $\widetilde{\mathbf{W}}, \widetilde{\mathbf{V}} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$ and implicitly sets

$$\mathbf{W} := \widetilde{\mathbf{W}} \left(\begin{array}{c|c} \mathbf{B}|b\cdot\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1} \text{ and } \mathbf{V} := \widetilde{\mathbf{V}} \left(\begin{array}{c|c} \mathbf{B}|b\cdot\mathbf{a}^\perp & 0 \\ \hline \mathbf{0} & 1 \end{array}\right)^{-1}.$$

Here we use the fact that $(\mathbf{B}|b\mathbf{a}^\perp)$ is full rank with probability $1 - \frac{1}{\Omega(p)}$ over over $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$, $\mathbf{a}^\perp \mathsf{orth}(\mathbf{A})$, and $b \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ (this is implied by Property 1).

Then, for $i \in [n], j \in [m]$, it computes

$$[\mathbf{c}_i]_1 := \left[\begin{pmatrix} \gamma\mathbf{r}_i \\ z\cdot x_i^{(b)} \\ 0 \end{pmatrix}^\top \left(\begin{array}{c|c|c} \mathbf{A}^\top\mathbf{B} & 0 & 0 \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \widetilde{\mathbf{W}}^{-1} \right]_1 \text{ and } [\widehat{\mathbf{c}}_j]_2 := \left[\widetilde{\mathbf{W}} \begin{pmatrix} \mathbf{s}_j \\ y_j^{(b)} \\ 0 \end{pmatrix} \right]_2$$

$$[\mathbf{c}_{n+i}]_1 := \left[\begin{pmatrix} \gamma\mathbf{r}_{n+i} \\ -z\cdot x_i^{(0)} \\ x_i^{(0)} \end{pmatrix}^\top \left(\begin{array}{c|c|c} \mathbf{A}^\top\mathbf{B} & 0 & 0 \\ \hline 0 & (\mathbf{b}^\perp)^\top\mathbf{a}^\perp & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \widetilde{\mathbf{V}}^{-1} \right]_1 \text{ and } [\widehat{\mathbf{c}}_{m+j}]_2 := \left[\widetilde{\mathbf{V}} \begin{pmatrix} \mathbf{s}_{m+j} \\ y_j^{(0)} \\ y_j^{(0)} \end{pmatrix} \right]_2.$$

Finally, $\mathcal{B}_3$ computes $[c_0]_1 := [\gamma]_1$, $[\widehat{c}_0]_2 := [\gamma]_2$, and simulates $\mathsf{KeyGenO}$ as in G_3 (see Figure 3.2). Note that when $[z]_1$ is a real 3-pddh challenge, i.e $[z]_1 = [abc]_1$, then $\mathcal{B}_3$ simulates game G_3; whereas it simulates game G_4 when $[z]_1 \leftarrow_{\mathrm{R}} \mathbb{G}_1$. This proves $|\mathsf{Adv}_3 - \mathsf{Adv}_4| \leq \mathbf{Adv}^{3-\mathsf{pddh}}_{\mathsf{GGen},\mathcal{B}_3}(\lambda) + 2^{-\Omega(\lambda)}$. □

Lemma 10 (G_4 *to* G_5)

There exist PPT adversaries $\mathcal{B}_4$ and $\mathcal{B}_5$ such that

$$|\mathsf{Adv}_4 - \mathsf{Adv}_5| \leq 2\cdot\mathbf{Adv}^{\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_1,\mathcal{B}_4}(\lambda) + 2\cdot\mathbf{Adv}^{\mathcal{D}_k\text{-mddh}}_{\mathsf{GGen},\mathbb{G}_2,\mathcal{B}_5}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof Lemma 10: This transition is symmetric to that between game G_0 and G_1: we use the selective, single-ciphertext security of the underlying private-key scheme (in Figure 1), to switch: $\{[\mathbf{A}\mathbf{r}_i + x_i^{(b)}\mathbf{b}^\perp]_1, [\mathbf{A}\mathbf{r}_{n+i} - x_i^{(0)}\mathbf{b}^\perp]_1, [\mathbf{B}\mathbf{s}_j + y_j^{(b)}\mathbf{a}^\perp]_2, [\mathbf{B}\mathbf{s}_{m+j} + y_j^{(0)}\mathbf{a}^\perp]_2\}_{i\in[n],j\in[m]}$ to $\{[\mathbf{A}\mathbf{r}_i]_1, [\mathbf{B}\mathbf{s}_j]_2\}_{i\in[2n],j\in[2m]}$, since $\mathbf{x}_i^{(b)\top}\mathbf{M}\mathbf{y}_j^{(b)} - \mathbf{x}_i^{(0)\top}\mathbf{M}\mathbf{y}_j^{(0)} = 0$, by definition of the security game. Thus, by Theorem 2 (security of the single-ciphertext secure scheme), we obtain the lemma. □

Theorem 4 follows from Lemmas 6-10, and the fact that game G_5 is independent from the bit $b \leftarrow_{\mathrm{R}} \{0,1\}$. □

4 Application to PE Supporting Degree-Two Polynomial Evaluation.

Here we show how to use our functional encryption schemes to build a Predicate Encryption (PE) scheme for the evaluation of bilinear maps over attributes. Specifically, we give a scheme

for the predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ where $\mathcal{X} \subset \mathbb{Z}_p^n \times \mathbb{Z}_p^m$, $\mathcal{Y} \subset \mathbb{Z}_p^{n \times m}$, and for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}$ and $\mathbf{M} \in \mathcal{Y}$:

$$\mathbf{x}^\top \mathbf{M} \mathbf{y} \in \{0,1\} \text{ and } \mathsf{P}((\mathbf{x}, \mathbf{y}), \mathbf{M}) = 1 \text{ iff } \mathbf{x}^\top \mathbf{M} \mathbf{y} = 1.$$

In Figure 7, we present a generic construction of PE for P from any functional encryption scheme FE for the bilinear maps functionality $F : \mathcal{K} \times \mathcal{M}' \to \mathcal{Y}'$, where $\mathcal{M}' := \mathbb{Z}_p^n \times \mathbb{Z}_p^m$, $\mathcal{K} := \mathbb{Z}_p^{n \times m}$, $\mathcal{Y}' := \mathbb{Z}_p$ and for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{M}'$, $\mathbf{M} \in \mathcal{K}$

$$F(\mathbf{M}, (\mathbf{x}, \mathbf{y})) = \mathbf{x}^\top \mathbf{M} \mathbf{y}.$$

The PE scheme can be instantiated by using one of our FE constructions presented in Sections 3.

$\underline{\mathsf{Setup}(1^\lambda, \mathsf{P}, \mathcal{M} := \mathbb{Z}_p):}$
Return $(\mathsf{pk}, \mathsf{msk}) \leftarrow_{\mathrm{R}} \mathsf{Setup}_{\mathsf{FE}}(1^\lambda, F)$

$\underline{\mathsf{KeyGen}(\mathsf{msk}, \mathbf{M} \in \mathcal{Y}):}$
Return $\mathsf{sk}_{\mathbf{M}} := \mathsf{KeyGen}_{\mathsf{FE}}(\mathsf{msk}, \mathbf{M})$

$\underline{\mathsf{Enc}(\mathsf{pk}, (\mathbf{x}, \mathbf{y}) \in \mathcal{X}, M \in \mathbb{Z}_p):}$
$w \leftarrow_{\mathrm{R}} \mathbb{Z}_p$; $C_0 := w + M$
$C_1 := \mathsf{Enc}_{\mathsf{FE}}(\mathsf{pk}, (w \cdot \mathbf{x}, \mathbf{y}))$
Return $\mathsf{ct}_{(\mathbf{x},\mathbf{y})} := (C_0, C_1)$

$\underline{\mathsf{Dec}(\mathsf{pk}, \mathsf{ct}_{(\mathbf{x},\mathbf{y})} := (C_0, C_1), \mathsf{sk}_{\mathbf{M}}):}$
$K := \mathsf{Dec}_{\mathsf{FE}}(\mathsf{pk}, C_1, \mathsf{sk}_{\mathbf{M}})$
Return $C_0 - K$.

Figure 7: PE, a predicate encryption scheme, selectively secure if the underlying FE scheme $(\mathsf{Setup}_{\mathsf{FE}}, \mathsf{KeyGen}_{\mathsf{FE}}, \mathsf{Enc}_{\mathsf{FE}}, \mathsf{Dec}_{\mathsf{FE}})$ is selectively secure.

Theorem 5 (*Correctness*)

If $\mathsf{FE} := (\mathsf{Setup}_{\mathsf{FE}}, \mathsf{KeyGen}_{\mathsf{FE}}, \mathsf{Enc}_{\mathsf{FE}}, \mathsf{Dec}_{\mathsf{FE}})$ *is a perfectly correct functional encryption scheme for functionality* F*, then so is the predicate encryption scheme* PE *defined in Figure 7.*

Proof Lemma 5: By correctness of FE, we have for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}$, $w \in \mathbb{Z}_p$, $\mathbf{M} \in \mathcal{Y}$:

$$F(\mathbf{M}, (w \cdot \mathbf{x}, \mathbf{y})) = w \cdot \mathbf{x}^\top \mathbf{M} \mathbf{y} = w \cdot \mathsf{P}((\mathbf{x}, \mathbf{y}), \mathbf{M}).$$

Thus, when $\mathsf{P}((\mathbf{x}, \mathbf{y}), \mathbf{M}) = 1$, decryption recovers the encapsulation key w. □

Theorem 6 (*Security*)

If $\mathsf{FE} := (\mathsf{Setup}_{\mathsf{FE}}, \mathsf{KeyGen}_{\mathsf{FE}}, \mathsf{Enc}_{\mathsf{FE}}, \mathsf{Dec}_{\mathsf{FE}})$ *is a selectively secure encryption scheme for* F*, then so is the predicate encryption scheme* PE *defined in Figure 7. Namely, for any PPT adversary* $\mathcal{A}$*, there exists a PPT adversary* $\mathcal{B}$ *such that:*

$$\mathsf{Adv}^{\mathsf{PE}}_{\mathcal{A}}(\lambda) \leq 4 \cdot \mathsf{Adv}^{\mathsf{FE}}_{\mathcal{B}}(\lambda).$$

Proof Lemma 6: We prove the selective security of PE via a series of games described in Figure 8 and we use Adv_i to denote the advantage of $\mathcal{A}$ in game G_i.

Lemma 11 ($\mathbf{G_0}$ *to* $\mathbf{G_1}$)

There exists a PPT adversary $\mathcal{B}_0$*:*

$$|\mathsf{Adv}_0 - \mathsf{Adv}_1| \leq 2 \cdot \mathsf{Adv}^{\mathsf{FE}}_{\mathcal{B}_0}(\lambda).$$

$\underline{\mathsf{SetupO}((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), M_0, (\mathbf{x}^{(1)}, \mathbf{y}^{(1)}), M_1)}$: $\quad$ $\mathrm{G}_0, \boxed{\mathrm{G}_1, \boxed{\mathrm{G}_2}}$:

$b \leftarrow_{\mathrm{R}} \{0,1\}$, $(\mathsf{pk}, \mathsf{msk}) \leftarrow_{\mathrm{R}} \mathsf{Setup}_{\mathsf{FE}}(1^\lambda, F)$
$w \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, $C_0 := w + M_b$, $C_1 := \mathsf{Enc}_{\mathsf{FE}}(\mathsf{pk}, (w \cdot \mathbf{x}^{(b)}, \mathbf{y}^{(b)}))$
$\boxed{\text{If } M_0 \neq M_1,\ C_1 := \mathsf{Enc}_{\mathsf{FE}}(\mathsf{pk}, (\mathbf{0}, \mathbf{0}))}$
$\boxed{\text{If } M_0 = M_1,\ C_1 := \mathsf{Enc}_{\mathsf{FE}}(\mathsf{pk}, (w \cdot \mathbf{x}^{(0)}, \mathbf{y}^{(0)}))}$
Return pk and $\mathsf{ct} := (C_0, C_1)$

$\underline{\mathsf{KeyGenO}(\mathbf{M} \in \mathbb{Z}_p^{n \times m})}$:
Return $\mathsf{sk}_{\mathbf{M}} := \mathsf{KeyGen}_{\mathsf{FE}}(\mathsf{msk}, \mathbf{M})$

Figure 8: Games G_i, for $i = 0, 1, 2$ for the proof of adaptive security of PE in Figure 7. In each procedure, the components inside a solid (dotted) frame are only present in the games marked by a solid (dotted) frame.

Proof Lemma 11: By definition of the security game, we know that if $M_0 \neq M_1$, then it must be that for all queries $\mathbf{M}$ to $\mathsf{KeyGenO}(\cdot)$, $\mathbf{x}^{(b)\top}\mathbf{M}\mathbf{y}^{(b)} = 0$ (i.e., the predicate over the challenge attributes is false). Therefore, using the security of the underlying FE scheme, we can switch: $\mathsf{Enc}(\mathsf{pk}, (w \cdot \mathbf{x}^{(b)}, \mathbf{y}^{(b)}))$, computed by SetupO when $M_0 \neq M_1$, to $\mathsf{Enc}(\mathsf{pk}, (\mathbf{0}, \mathbf{0}))$. □

Lemma 12 ($\mathbf{G_1}$ *to* $\mathbf{G_2}$)

There exists a PPT adversary $\mathcal{B}_1$:

$$|\mathsf{Adv}_1 - \mathsf{Adv}_2| \leq 2 \cdot \mathsf{Adv}^{\mathsf{FE}}_{\mathcal{B}_1}(\lambda).$$

Proof Lemma 12: By definition of the security game, we know that for all queries $\mathbf{M}$ to $\mathsf{KeyGenO}(\cdot)$, $\mathsf{P}\big((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), \mathbf{M}\big) = \mathsf{P}\big((\mathbf{x}^{(1)}, \mathbf{y}^{(1)}), \mathbf{M}\big)$. Together with the fact that for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}$ and $\mathbf{M} \in \mathcal{Y}$: $\mathbf{x}^\top \mathbf{M} \mathbf{y} \in \{0, 1\}$, we obtain that: $\mathbf{x}^{(0)\top}\mathbf{M}\mathbf{y}^{(0)} = \mathbf{x}^{(1)\top}\mathbf{M}\mathbf{y}^{(1)}$. Therefore, using the security of the underlying FE scheme, we can switch: $\mathsf{Enc}(\mathsf{pk}, (w \cdot \mathbf{x}^{(b)}, \mathbf{y}^{(b)}))$, computed by SetupO when $M_0 = M_1$, to $\mathsf{Enc}(\mathsf{pk}, (w \cdot \mathbf{x}^{(0)}, \mathbf{y}^{(0)}))$. □

Lemma 13 ($\mathbf{G_2}$)

$\mathsf{Adv}_2 = 0$.

Proof Lemma 13: We show that the $\mathcal{A}$'s view is independent of $b \leftarrow_{\mathrm{R}} \{0, 1\}$ in this game. If $M_0 \neq M_1$, the challenge ciphertext is of the form (C_0, C_1) where $C_0 := [w]_T + M_b$ for $w \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, and C_1 is independent of w and b. Thus, the message M_b is completely hidden by the one-time pad $[w]_T$, and the ciphertext is independent of b.

If $M_0 = M_1$, the challenge ciphertext is of the form (C_0, C_1) where $C_0 := [w]_T + M_b$ for $w \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, which is independent of b since $M_0 = M_1$; and $C_1 := \mathsf{Enc}(\mathsf{pk}, (w \cdot \mathbf{x}^{(0)}, \mathbf{y}^{(0)}))$, which is also independent of b. □

Theorem 6 follows readily from Lemmas 11, 12, and 13. □

4.1 Applications of PE for Bilinear Maps Evaluation

In this section, we discuss two applications of our fully attribute-hiding PE scheme supporting bilinear maps evaluation.

PE for constant depth boolean formulas.

As a first application, we can use the PE scheme in Figure 7 to handle boolean functions of constant degree d in n variables. This yields a solution where ciphertexts comprise $O(n^{d/2})$ group elements, in contrast to $O(n^d)$ group elements in [26] (the asymptotic is taken for large n, constant d).

The idea is to encode a predicate for boolean formulas into a predicate for bilinear maps evaluation. This can be done as follows. Consider the following predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$, with $\mathcal{X} := \mathbb{Z}_2^n$ and $\mathcal{Y} := \{T \in \mathbb{Z}_2[X_1, \ldots, X_n], \deg(T) \leq d\}$, such that for all $\mathbf{x} \in \mathcal{X}$, $T \in \mathcal{X}$, $\mathsf{P}(\mathbf{x}, T) = 1$ iff $T(\mathbf{x}) = 1$. Below we describe how to encode $\mathbf{x} \in \mathcal{X}$ and $T \in \mathcal{Y}$ into a vector $\widetilde{\mathbf{x}}$ and a matrix $\widetilde{\mathbf{T}}$ such that $\mathsf{P}(\mathbf{x}, T) = 1$ iff $\widetilde{\mathbf{x}}^\top \widetilde{\mathbf{T}} \widetilde{\mathbf{x}} = 1$.

To see this, assume for simplicity that d is even, and let us consider the setting where $n \geq \frac{d}{2}$. First, we map every $\mathbf{x} \in \mathcal{X}$ to $\widetilde{\mathbf{x}} := (M_1(\mathbf{x}), \ldots, M_{\widetilde{d}}(\mathbf{x})) \in \mathbb{Z}_2^{\widetilde{d}}$, where $\widetilde{d} := \sum_{i=0}^{\frac{d}{2}} \binom{n}{i}$, and for all $j \in \left[\binom{n}{\frac{d}{2}}\right]$, M_j is the j-th monomial of degree at most $\frac{d}{2}$ on n variables (there are exactly $\widetilde{d}$ such monomials, which we order arbitrarily). Second, we write every $T \in \mathcal{Y}$ as $\sum_{i,j \in [\widetilde{d}]} T_{i,j} M_i M_j$, where for all $i, j \in [\widetilde{d}]$, $T_{i,j} \in \mathbb{Z}_2$, and we map $T \in \mathcal{Y}$ to $\widetilde{\mathbf{T}} \in \mathbb{Z}_2^{\widetilde{d} \times \widetilde{d}}$ such that for all $i, j \in [\widetilde{d}]$, $\widetilde{T}_{i,j} := T_{i,j}$. This way, for all $\mathbf{x} \in \mathcal{X}$ and $T \in \mathcal{Y}$, we have $\mathsf{P}(\mathbf{x}, T) = 1$ iff $\widetilde{\mathbf{x}}^\top \widetilde{\mathbf{T}} \widetilde{\mathbf{x}} = T(\mathbf{x}) = 1$.

Therefore, using the PE which supports bilinear maps evaluation presented in Section 4, we obtain a PE for boolean formulas with ciphertexts of size $O(\widetilde{d})$. Using a similar encoding to the PE from [26] that support linear maps evaluation yields a solution with ciphertexts of dimension $O(\widehat{d})$ where $\widehat{d} := \sum_{i=0}^{d} \binom{n}{i}$. When considering asymptotic for large n, constant d, our ciphertext size is $O(n^{d/2})$, against $O(n^d)$ for [26].

Finally, we note that boolean formulas can be arithmetized into a polynomial over $\mathbb{Z}_2$, à la [34]. Namely, for boolean variables $x, y \in \mathbb{Z}_2$, $\mathsf{AND}(x, y)$ is encoded as $x \cdot y$, $\mathsf{OR}(x, y)$ is encoded as $x + y - xy$, and $\mathsf{NOT}(x) = 1 - x$.

PE for comparison.

Let us consider the comparison predicate $\mathsf{P}_{\leq} : [N] \times [N] \to \{0,1\}$ that for all $x, y \in [N]$ is defined by

$$\mathsf{P}_{\leq}(x, y) = 1 \text{ iff } x \leq y.$$

We can reduce this predicate to a polynomial of degree two, as done (implicitly) in [10], as follows. First, any integer $x \in [N]$ is canonically mapped to the lexicographically ordered pair $(x_1, x_2) \in [\sqrt{N}] \times [\sqrt{N}]$ (we assume $\sqrt{N}$ is an integer for simplicity). Then x_1 is mapped to vectors $\widetilde{\mathbf{x}} := \begin{pmatrix} \mathbf{0}^{x_1} \\ \mathbf{1}^{\sqrt{N}-x_1} \end{pmatrix} \in \{0,1\}^{\sqrt{N}}$ where $\mathbf{1}^\ell$, $\mathbf{0}^\ell$ denote the all-one and all-zero vectors in $\{0,1\}^\ell$, respectively; and $\widehat{\mathbf{x}} := \mathbf{e}_{x_1} \in \{0,1\}^{\sqrt{N}}$, where for all $i \in [\sqrt{N}]$, $\mathbf{e}_i$ denotes the i'th vector of the canonical basis of $\mathbb{Z}_p^{\sqrt{N}}$. Finally, $x_2 \in [\sqrt{N}]$ is mapped to $\bar{\mathbf{x}} := \begin{pmatrix} \mathbf{0}^{x_2-1} \\ \mathbf{1}^{\sqrt{N}-x_2+1} \end{pmatrix}$. For all $(x_1, x_2), (y_1, y_2) \in [\sqrt{N}] \times [\sqrt{N}]$:

$$\mathsf{P}_{\leq}((x_1, x_2), (y_1, y_2)) = 1 \text{ iff } \widetilde{x}_{y_1} + \widehat{x}_{y_1} \cdot \bar{x}_{y_2} = 1,$$

where for any vector $\mathbf{z} \in \mathbb{Z}_p^{\sqrt{N}}$, and any $i \in [\sqrt{N}]$, we denote by $z_i \in \mathbb{Z}_p$ the i-th coordinate of $\mathbf{z}$.

This means that by using the above encoding, for an integer attribute $x \in [N]$ one can use a PE for bilinear maps evaluation to encrypt the pair of vectors

$$\left(\begin{pmatrix}\widetilde{\mathbf{x}}\\ \widehat{\mathbf{x}}\end{pmatrix}, \begin{pmatrix}1\\ \bar{\mathbf{x}}\end{pmatrix}\right) \in \mathbb{Z}_p^{2\sqrt{N}} \times \mathbb{Z}_p^{1+\sqrt{N}}$$

This gives a PE for comparison with ciphertexts of $O(\sqrt{N})$ group elements, as in [10, 21]. More precisely, by instantiating our PE scheme with the FE of Section 3.2, we obtain a PE for comparison with ciphertext size $(12\sqrt{N}+1)\cdot|\mathrm{G}_1| + (6\sqrt{N}+7)\cdot|\mathrm{G}_2|$, and secret-key size $|\mathrm{G}_1|+|\mathrm{G}_2|$, compared to ciphertext size $5\sqrt{N}\cdot|\mathrm{G}_1|+4\sqrt{N}\cdot|\mathrm{G}_2|+|\mathrm{G}_T|$ and secret-key size $|\mathrm{G}_2|$ for [21], where both schemes are selectively-secure based on SXDH.

Acknowledgments.

We would like to thank Florian Bourse, Alain Passelègue, and Hoeteck Wee for insightful discussions.

References

[1] M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval. Simple functional encryption schemes for inner products. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 733–751. Springer, Mar. / Apr. 2015. 1, 2, 4

[2] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 553–572. Springer, May 2010. 2

[3] S. Agrawal, B. Libert, and D. Stehlé. Fully secure functional encryption for inner products, from standard assumptions. LNCS, pages 333–362. Springer, Aug. 2016. 1, 2, 4

[4] P. Ananth and A. Jain. Indistinguishability obfuscation from compact functional encryption. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part I*, LNCS, pages 308–326. Springer, Aug. 2015. 1

[5] P. Ananth, A. Jain, and A. Sahai. Indistinguishability obfuscation from functional encryption for simple functions. Cryptology ePrint Archive, Report 2015/730, 2015. http://eprint.iacr.org/2015/730. 1

[6] P. Ananth and A. Sahai. Projective arithmetic functional encryption and indistinguishability obfuscation from degree-5 multilinear maps. In *EUROCRYPT*, 2017. 5

[7] N. Attrapadung, G. Hanaoka, and S. Yamada. A framework for identity-based encryption with almost tight security. LNCS, pages 521–549. Springer, Dec. 2015. 2

[8] N. Bitansky and V. Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In *56th FOCS*, pages 171–190. IEEE Computer Society Press, 2015. 1

[9] O. Blazy, E. Kiltz, and J. Pan. (Hierarchical) identity-based encryption from affine message authentication. In J. A. Garay and R. Gennaro, editors, *CRYPTO 2014, Part I*, volume 8616 of *LNCS*, pages 408–425. Springer, Aug. 2014. 2

[10] D. Boneh, A. Sahai, and B. Waters. Fully collusion resistant traitor tracing with short ciphertexts and private keys. In S. Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 573–592. Springer, May / June 2006. 1, 2, 4, 5, 7, 23, 24

[11] D. Boneh, A. Sahai, and B. Waters. Functional encryption: Definitions and challenges. In Y. Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273. Springer, Mar. 2011. 1

[12] D. Boneh and B. Waters. A fully collusion resistant broadcast, trace, and revoke system. In A. Juels, R. N. Wright, and S. Vimercati, editors, *ACM CCS 06*, pages 211–220. ACM Press, Oct. / Nov. 2006. 2, 4, 5

[13] X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In C. Dwork, editor, *CRYPTO 2006*, volume 4117 of *LNCS*, pages 290–307. Springer, Aug. 2006. 2

[14] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 523–552. Springer, May 2010. 2

[15] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert. Bonsai trees, or how to delegate a lattice basis. *Journal of Cryptology*, 25(4):601–639, Oct. 2012. 2

[16] J. Chen, R. Gay, and H. Wee. Improved dual system ABE in prime-order groups via predicate encodings. In E. Oswald and M. Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 595–624. Springer, Apr. 2015. 3, 6

[17] J. Chen, H. W. Lim, S. Ling, H. Wang, and H. Wee. Shorter IBE and signatures via asymmetric pairings. In M. Abdalla and T. Lange, editors, *PAIRING 2012*, volume 7708 of *LNCS*, pages 122–140. Springer, May 2013. 2, 5

[18] P. Datta, R. Dutta, and S. Mukhopadhyay. Functional encryption for inner product with full function privacy. LNCS, pages 164–195. Springer, 2016. 5

[19] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie-Hellman assumptions. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 129–147. Springer, Aug. 2013. 2, 3, 6, 7

[20] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *54th FOCS*, pages 40–49. IEEE Computer Society Press, Oct. 2013. 1

[21] S. Garg, A. Kumarasubramanian, A. Sahai, and B. Waters. Building efficient fully collusion-resilient traitor tracing and revocation schemes. In E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, editors, *ACM CCS 10*, pages 121–130. ACM Press, Oct. 2010. 2, 4, 5, 24

[22] R. Gay, P. Méaux, and H. Wee. Predicate encryption for multi-dimensional range queries from lattices. In J. Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 752–776. Springer, Mar. / Apr. 2015. 2

[23] S. Gorbunov, V. Vaikuntanathan, and H. Wee. Predicate encryption for circuits from LWE. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part II*, LNCS, pages 503–523. Springer, Aug. 2015. 2

[24] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-based encryption for fine-grained access control of encrypted data. In A. Juels, R. N. Wright, and S. Vimercati, editors, *ACM CCS 06*, pages 89–98. ACM Press, Oct. / Nov. 2006. Available as Cryptology ePrint Archive Report 2006/309. 1

[25] A. Guillevic. Comparing the pairing efficiency over composite-order and prime-order elliptic curves. In M. J. Jacobson Jr., M. E. Locasto, P. Mohassel, and R. Safavi-Naini, editors, *ACNS 13*, volume 7954 of *LNCS*, pages 357–372. Springer, June 2013. 4

[26] J. Katz, A. Sahai, and B. Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In N. P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 146–162. Springer, Apr. 2008. 1, 2, 23

[27] A. B. Lewko. Tools for simulating features of composite order bilinear groups in the prime order setting. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 318–335. Springer, Apr. 2012. 5

[28] A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 62–91. Springer, May 2010. 2

[29] H. Lin. Indistinguishability obfuscation from DDH on 5-linear maps and locality-5 prgs. *IACR Cryptology ePrint Archive*, 2016:1096, 2016. 5

[30] T. Okamoto and K. Takashima. Homomorphic encryption and signatures from vector decomposition. In S. D. Galbraith and K. G. Paterson, editors, *PAIRING 2008*, volume 5209 of *LNCS*, pages 57–74. Springer, Sept. 2008. 5

[31] T. Okamoto and K. Takashima. Hierarchical predicate encryption for inner-products. In M. Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 214–231. Springer, Dec. 2009. 2, 5

[32] T. Okamoto and K. Takashima. Adaptively attribute-hiding (hierarchical) inner product encryption. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 591–608. Springer, Apr. 2012. 2

[33] A. Sahai and B. R. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 457–473. Springer, May 2005. 1

[34] A. Shamir. IP=PSPACE. In *31st FOCS*, pages 11–15. IEEE Computer Society Press, Oct. 1990. 23

[35] E. Shi, J. Bethencourt, H. T.-H. Chan, D. X. Song, and A. Perrig. Multi-dimensional range query over encrypted data. In *2007 IEEE Symposium on Security and Privacy*, pages 350–364. IEEE Computer Society Press, May 2007. 2

[36] J. Tomida, M. Abe, and T. Okamoto. Efficient functional encryption for inner-product values with full-hiding security. In *Information Security - 19th International Conference, ISC 2016, Honolulu, HI, USA, September 3-6, 2016, Proceedings*, pages 408–425, 2016. 5

[37] B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 619–636. Springer, Aug. 2009. 5

[38] H. Wee. Déjà Q: Encore! Un petit IBE. LNCS, pages 237–258. Springer, 2016. 2