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 [24] and [9].

1 Introduction

Functional Encryption [10](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 [7, 4, 5] proves that an FE for sufficiently general functions[1] gives a construction for the almighty Indistinguishability Obfuscation for circuits [19]. 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 [24](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 [30, 23] 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.

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

[*] Supported by ERC Project aSCEND (639554).

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

set of values, and secret keys are associated with a degree-two polynomial. This way, the decryption of a ciphertext $\mathsf{ct}_{(x_1,\dots,x_n)\in\mathbb{Z}_p^n}$ with a secret key $\mathsf{sk}_{P\in\mathbb{Z}_p[X_1,\dots,X_n],\mathsf{deg}(P)\leq 2}$ recovers $P(x_1,\dots,x_n)$. 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 $\mathsf{ct}_{(x_1,\dots,x_n)\in\mathbb{Z}_p^n}$ with a secret key $\mathsf{sk}_{P\in\mathbb{Z}_p[X_1,\dots,X_n],\ \mathsf{deg}(P)\leq 2}$ recovers the plaintext if, and only if, $P(x_1,\dots,x_n)=1$. The attribute-hiding property refers to the fact that $\mathsf{ct}_{(x_1,\dots,x_n)\in\mathbb{Z}_p^n}$ leaks no information on its attribute $(x_1,\dots,x_n)$, beyond the inherent leakage of the boolean value $P(x_1,\dots,x_n)=1$. Again, this is done with ciphertexts of $O(n)$ group elements, instead of $O(n^2)$ when using [24], 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 [18], which generalizes standard assumptions such as DLIN or k-Lin for $k \geq 1$, and the 3-pddh assumption [9].

Comparison with prior works. Prior PE schemes based on standard assumptions exist for Identity-Based Encryption [12,2,8,6,13,35] (in this context, the attribute-hiding property is referred to as anonymity of the IBE), Inner Product Encryption [24,28,26,29,14,16], and comparison [9,11,20], 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 [22], or PE for comparison with $O(\log n)$ group elements per ciphertext [32,21]. 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 $\mathsf{ct}_{(x_1,\dots,x_n)}$ of $O(n)$ group elements, that must hide their attribute $(x_1,\dots,x_n)\in\mathbb{Z}_p^n$, 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 $e:\mathbb{G}_1\times\mathbb{G}_2\rightarrow\mathbb{G}_T$, 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: $\mathcal{X}:=\mathbb{Z}_p^n\times\mathbb{Z}_p^m$, $\mathcal{K}:=\mathbb{Z}_p^{n\cdot m}$, and for all $(\mathbf{x},\mathbf{y})\in\mathcal{X}$, $\alpha\in\mathcal{K}$,

$$F((\mathbf{x},\mathbf{y}),\alpha)=\sum_{i\in[n],j\in[m]}\alpha_{i,j}x_iy_j.$$

Private-key, single-ciphertext secure FE. Our starting point is a private-key FE for the boolean function defined for $(\mathbf{x},\mathbf{y})\in\mathcal{X}$ and $\alpha\in\mathcal{Y}$ by $F((\mathbf{x},\mathbf{y}),\alpha)=0$ (that is, decryption only gets to know whether $F((\mathbf{x},\mathbf{y}),\alpha)$ is 0 or not, but not the exact value), that is only secure for a single-ciphertext:

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

where we rely on implicit representation notation [18] 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 [15]. 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 sk_α. Correctness follows from the orthogonal property: decryption computes $\sum_{i,j} \alpha_{i,j} e([\mathbf{A}\mathbf{r}_i + \mathbf{b}^\perp x_i]_1^\top, [\mathbf{B}\mathbf{s}_j + \mathbf{a}^\perp y_j]_2) = \mathsf{sk}_\alpha + (\mathbf{a}^\perp)^\top\mathbf{b}^\perp \cdot [F((\mathbf{x},\mathbf{y}),\alpha)]_T$ which is equal to sk_α if, and only if, $F((\mathbf{x},\mathbf{y}),\alpha) = 0$. Security relies on the $\mathcal{D}_k$-mddh Assumption [18], 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 $\mathbf{r}, \mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$. 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 $\left[\sum_{i,j} \alpha_{i,j} x_i^1 y_j^1 - \sum_{i,j} \alpha_{i,j} x_i^0 y_j^0\right]_T$ in the secret keys sk_α. We conclude the proof using the fact that for all α queried to KeyGen, $F((\mathbf{x}^0, \mathbf{y}^0), \alpha) = F((\mathbf{x}^1, \mathbf{y}^1), \alpha)$, as required by the security definition for FE (see Section 2.4 for the definition of FE), which cancels out the extra term in all secret keys.

Going from one to many challenge ciphertexts poses three problems.

1. 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 $\mathsf{sk}_\alpha := [\mathbf{r}_1^\top\mathbf{A}^\top\mathbf{B}\mathbf{s}_1]_T$ for $\alpha = 1$, 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.
2. 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 $[\mathbf{b}^\perp]_1$ needs to be part of the public key.
3. In the public-key setting, the secret keys sk_α for all α are computable efficiently from the public key that contains the vectors $[\mathbf{A}\mathbf{r}_i]_1$, $[\mathbf{B}\mathbf{s}_j]_2$.

To solve 1., we randomize the encryption by randomizing the bases $(\mathbf{A}|\mathbf{b}^\perp)$ and $(\mathbf{B}|\mathbf{a}^\perp)$ into $\mathbf{W}^{-1}(\mathbf{A}|\mathbf{b}^\perp)$ and $\mathbf{W}^\top(\mathbf{B}|\mathbf{a}^\perp)$ for $\mathbf{W} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+1}$ a random invertible matrix. This "glues" the components of a ciphertext that are in $\mathbb{G}_1$ to those that are in $\mathbb{G}_2$.

To solve 2., we add an extra dimension, namely, we draw $[\mathbf{A}]_1$ and $[\mathbf{B}]_2$ from matrix distributions over $\mathbb{Z}_p^{(k+2)\times k}$, and we use bases $(\mathbf{A}|\mathbf{b}^\perp|\mathbf{c})$ and $(\mathbf{B}|\mathbf{a}^\perp|\mathbf{d})$ where $\mathbf{c}$ and $\mathbf{d}$ 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). For correctness to hold, we require that $\mathbf{c}$ is orthogonal to $(\mathbf{B}|\mathbf{a}^\perp)$, and $\mathbf{d}$ to $(\mathbf{A}|\mathbf{b}^\perp)$. Note that this is different from the previous scheme, where the vectors $\mathbf{a}^\perp$ and $\mathbf{b}^\perp$ were used both for security and correctness. Here, knowing the vectors $\mathbf{c}$ and $\mathbf{d}$, as required by correctness, a priori is not incompatible with the MDDH assumption on $[\mathbf{A}]_1$ and $[\mathbf{B}]_2$.

Finally, to solve 3., we generate secret keys in $\mathbb{G}_2$ instead of $\mathbb{G}_T$, namely $\mathsf{sk}_\alpha := [\sum_{i,j} \alpha_{i,j}\mathbf{r}_i^\top\mathbf{A}^\top\mathbf{B}\mathbf{s}_j]_2$. 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 $[F((\mathbf{x},\mathbf{y}),\alpha)]_T + [\gamma\sigma \cdot \sum_{i,j} \alpha_{i,j}\mathbf{r}_i^\top\mathbf{A}^\top\mathbf{B}\mathbf{s}_j]_T$, where the second term of the sum is $e([\gamma\sigma]_1, \mathsf{sk}_\alpha)$. Including this "quadratic information" $[\gamma \cdot \sigma]_2$ inside the ciphertexts is similar to the techniques used originally in [9], and in follow up [11, 20]. 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.

Combining the solutions to 1., 2., and 3., we obtain:

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

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

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

Then, to get back the value $F((\mathbf{x},\mathbf{y}),\alpha)$ in $\mathbb{Z}_p$ (and not only the boolean $F((\mathbf{x},\mathbf{y}),\alpha) = 0$), 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].

Finally, to use asymmetric pairings, we secret share the secret keys sk_αin two group elements, one in $\mathbb{G}_1$, and the other in $\mathbb{G}_2$, such that either $[\mathbf{A}^\top\mathbf{B}]_1$ or $[\mathbf{A}^\top\mathbf{B}]_2$ is needed to simulate sk_α at some point in the security proof, but never both. This allows to use mddh alternatively in $\mathbb{G}_1$ or $\mathbb{G}_2$.

Discussion. The scheme described above is identically distributed than

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

$$\mathsf{sk}_\alpha := [\sum_{i,j} \alpha_{i,j} \mathbf{r}_i^\top \mathbf{s}_j]_2,$$

which is like the Dual Pairing Vector Space constructions, originally introduced in [27], and later used in [28, 25, 16] in the context of attribute-based encryption, and in [17, 33] in the context of FE for inner product, with the crucial difference the all these previous construction 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 [34], 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 [9] and follow-up works [11, 20] 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. With this construction, 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.

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 new PE that support degree-two polynomial evaluation, and other interesting predicates, such as comparison.

2 Preliminaries

2.1 Notations

We denote by $s \leftarrow_{\mathrm{R}} S$ the fact that s is picked uniformly at random from a finite set S. By PPT, we denote a probabilistic polynomial-time algorithm. Throughout this paper, we use 1^λ as the security parameter. We use $\cdot$ to denote multiplication as well as component-wise multiplication. We denote by λ the security parameter, and by $\mathsf{negl}(\cdot)$ any negligible function of λ.

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 [18].

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

Property 1 (Basis property).

$$\Pr[(\mathbf{A}|\mathbf{b}^\perp) \textit{ and } (\mathbf{B}|\mathbf{a}^\perp) \textit{ are full rank }] = 1 - \frac{1}{\Omega(p)},$$

where $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k, \mathbf{a}^\perp, \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ such that $\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{B}^\top \mathbf{b}^\perp = \mathbf{0}$.

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 [18], but, as noted in [15, Lemma 1 (basis lemma)], all examples of matrix distribution presented in [18, 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 $\mathcal{A}$,*

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

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 $k \geq 1$, [18] 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.

We also recall the definition of 3-party Decision Diffie-Hellman (3-pddh) Assumption introduced in [9]. 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 $\mathcal{A}$,*

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

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 ($\mathsf{Setup}, \mathsf{Enc}, \mathsf{KeyGen}, \mathsf{Dec}$):

$\mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{K}, \mathcal{Y}) \to (\mathsf{pk}, \mathsf{msk}, \mathsf{ek})$. 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. Note that k is public given sk_k.

$\mathsf{Dec}(\mathsf{pk}, \mathsf{sk}_k, \mathsf{ct}_x) \to y$. The decryption algorithm gets as input sk_k and ct_x. It outputs $y \in \mathcal{Y}$.

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

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

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.

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

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

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 $\mathsf{Adv}^{\mathsf{FE}}_{\mathcal{A}}(\lambda)$ is a negligible function in λ. 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. Note that y is public given sk_y.

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

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

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

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.

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

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

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 $n \in \mathbb{N}$, $\mathcal{PG} = (p, \mathbb{G}_1, \mathbb{G}_2, P_1, P_2, \mathbb{G}_T, e) \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathcal{X} \subset \mathbb{Z}_p^n \times \mathbb{Z}_p^m$, $\mathcal{K} \subset \mathbb{Z}_p^{n \cdot m}$, $\mathcal{Y} := F(\mathcal{X}, \mathcal{K}) \subset \mathbb{G}_T$, and for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}$, $\alpha \in \mathcal{K}$:

$$F((\mathbf{x}, \mathbf{y}), \alpha) = \left[\sum_{i \in [n], j \in [m]} \alpha_{i,j} x_i y_j \right]_T \in \mathbb{G}_T$$

Remark 2 ($\mathcal{Y} = \mathbb{Z}_p$). Note that we can build a scheme for any $\mathcal{X} \subset \mathbb{Z}_p^n \times \mathbb{Z}_p^m$,$\mathcal{K} \subset \mathbb{Z}_p^{n \cdot m}$, $\mathcal{Y} := F(\mathcal{X}, \mathcal{K}) \subset \mathbb{Z}_p$ where for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}$, $\alpha \in \mathcal{K}$:

$$F((\mathbf{x}, \mathbf{y}), \alpha) = \sum_{i \in [n], j \in [m]} \alpha_{i,j} x_i y_j \mod p,$$

as long as $|\mathcal{Y}|$ is polynomial in the security parameter, using a look-up table to recover $\sum_{i \in [n], j \in [m]} \alpha_{i,j} x_i y_j \mod p$ from $\left[\sum_{i \in [n], j \in [m]} \alpha_{i,j} x_i y_j\right]_T$.

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, for the boolean function which for all $(\mathbf{x}, \mathbf{y}) \in \mathcal{X}$, $\alpha \in \mathcal{K}$, returns the boolean value:

$$F((\mathbf{x}, \mathbf{y}), \alpha) = [0]_T,$$

where F is defined above. In Section 3.2, we build up from the latter a public-key functional encryption for F.

3.1 Private-key, Single-ciphertext secure FE

In Figure 3.1, 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 3.1 is single-ciphertext, selectively secure under the $\mathcal{D}_k$-mddh assumption, on asymmetric pairings.

Theorem 1 (Correctness). *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 Figure 3.1 has perfect correctness.*

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

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

```
$\mathsf{Setup}(1^\lambda, \mathcal{X}, \mathcal{K}, \mathcal{Y}, 1^k, \mathcal{D}_k)$:
$\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$, $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$; $\mathbf{a}^\perp, \mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ s.t. $\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{B}^\top \mathbf{b}^\perp = \mathbf{0}$
For $i \in [n], j \in [m]$, $\mathbf{r}_i, \mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$.
Return $\mathsf{pk} := \mathcal{PG}$ and
$\mathsf{msk} := \left(\mathbf{A}, \mathbf{a}^\perp, \mathbf{B}, \mathbf{b}^\perp, \{\mathbf{r}_i, \mathbf{s}_j\}_{i \in [n], j \in [m]}\right)$

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

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

$\mathsf{Dec}(\mathsf{pk}, \mathsf{ct}_{(\mathbf{x},\mathbf{y})}, \mathsf{sk}_\alpha)$:
Return the boolean: $\sum_{i \in [n], j \in [m]} \alpha_{i,j} \cdot e(C_i, \widehat{C}_j) = e(K, [1]_2) + e([1]_1, \widehat{K})$.
```

Fig. 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.

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

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

The basis property (Property 1 in Definition 1) implies that $(\mathbf{a}^\perp)^\top \mathbf{b}^\perp \neq 0$, which allows to check if $\sum_{i,j} \alpha_{i,j} x_i y_j$ is 0. □

Theorem 2 (Security). *For any $k \in \mathbb{N}^*$ and any matrix distribution $\mathcal{D}_k$, if the $\mathcal{D}_k$-mddh assumptions hold in $\mathcal{PG}$, then the functional encryption scheme $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$ defined in Figure 3.1 is selectively secure, in a single-ciphertext setting (see the security definition in Section 2.4). Namely, for any adversary $\mathcal{A}$, there exists adversaries $\mathcal{B}$ such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A})$ and*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{FE}_{\mathsf{one}}}(\lambda) \leq 3 \cdot \mathbf{Adv}_{\mathsf{GGen}, \mathcal{B}}^{\mathcal{D}_k\text{-}\mathsf{mddh}}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof of Theorem 2. We prove the security of $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$ via a series of games described in Figure 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, in the private-key, single-ciphertext setting, as defined in Section 2.4.

Lemma 1 (G_0 to G_1). *There exists an adversary $\mathcal{B}_0$ such that $\mathbf{T}(\mathcal{B}_0) \approx \mathbf{T}(\mathcal{A})$ and*

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

Proof of Lemma 1. 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 $[\mathbf{A}]_2$.

First, we use the fact that for any vector $\mathbf{a}^\perp$ orthogonal to $\mathbf{A}$, we have :

$$\sum_{i,j} \alpha_{i,j} \mathbf{r}_i^\top \mathbf{A}^\top \mathbf{B} \mathbf{s}_j = \sum_{i,j} \alpha_{i,j} \big(\mathbf{A}\mathbf{r}_i + \boxed{x_i^{(b)} \mathbf{b}^\perp}\big)^\top \big(\mathbf{B}\mathbf{s}_j + \boxed{y_j^{(b)} \mathbf{a}^\perp}\big) - \boxed{\sum_{i,j} \alpha_{i,j} x_i^{(b)} (\mathbf{b}^\perp)^\top (\mathbf{B}\mathbf{s}_j + y_j^{(b)} \mathbf{a}^\perp)}.$$

Then, we switch $\{\mathbf{B}\mathbf{s}_j + y_j^{(b)} \mathbf{a}^\perp\}_{j \in [m]}$ to $\{\mathbf{B}\mathbf{s}_j + y_j^{(b)} \mathbf{z}\}_{j \in [m]}$, where $\mathbf{z} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$. This allows to simulate SetupO and $\mathsf{KeyGenO}$ without knowing $\mathbf{a}^\perp$. This is justified by the fact that $\{\mathbf{s}_j\}_{j \in [m]}$

```
$\underline{\mathsf{SetupO}\big((\mathbf{x}^{(0)},\mathbf{y}^{(0)}),(\mathbf{x}^{(1)},\mathbf{y}^{(1)})\big)}$:      $G_0$, $\boxed{G_1, \boxed{G_2}}$
$\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$; $\mathbf{A},\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$; $b \leftarrow_{\mathrm{R}} \{0,1\}$; $\mathbf{a}^\perp,\mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ s.t. $\mathbf{A}^\top\mathbf{a}^\perp = \mathbf{B}^\top\mathbf{b}^\perp = \mathbf{0}$
For $i \in [n], j \in [m]$: $\mathbf{r}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$
$C_i := [\mathbf{Ar}_i + x_i^{(b)}\mathbf{b}^\perp]_1$; $\boxed{C_i := [\mathbf{Ar}_i]_1}$
$\widehat{C}_j := [\mathbf{Bs}_j + y_i^{(b)}\mathbf{a}^\perp]_2$; $\boxed{\widehat{C}_j := [\mathbf{Bs}_j]_2}$
Return $\mathsf{ct}_{(\mathbf{x},\mathbf{y})} := \{C_i, \widehat{C}_j\}_{i\in[n],j\in[m]}$

$\underline{\mathsf{KeyGenO}(\alpha \in \mathbb{Z}_p^{n\cdot m})}$:
$K := [u]_1 \leftarrow_{\mathrm{R}} \mathbb{G}_1$; $\widehat{K} := [\sum_{i,j}\alpha_{i,j}\mathbf{r}_i^\top\mathbf{A}^\top\mathbf{Bs}_j]_2 - [u]_2 - \boxed{(\mathbf{b}^\perp)^\top\mathbf{a}^\perp \cdot [\sum_{i,j}\alpha_{i,j}x_i^{(b)}y_j^{(b)}]_2}$
Return $\mathsf{sk}_\alpha := (K, \widehat{K})$
```

Fig. 2. Games G_0, G_1, G_2 for the proof of selective security of $\mathsf{FE}_{\mathsf{one}}(k, \mathcal{D}_k)$ in Figure 3.1. In each procedure, the components inside a solid (dotted, gray) frame are only present in the games marked by a solid (dotted, gray) frame.

and $\{\mathbf{s}_j + y_j^{(b)}\mathbf{s}\}_{j\in[m]}$ are identically distributed for $\mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, so we can write $\mathbf{Bs}_j + y_j^{(b)}\mathbf{a}^\perp$ as $\mathbf{Bs}_j + y_j^{(b)}(\mathbf{Bs} + \mathbf{a}^\perp)$; then, we use the fact that $\mathbf{a}^\perp$ is identically distributed as $\widetilde{s}\widetilde{\mathbf{a}^\perp}$, where $\widetilde{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^*$ and $\widetilde{\mathbf{a}^\perp} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ such that $\mathbf{A}^\top\widetilde{\mathbf{a}^\perp} = \mathbf{0}$; then, we use the fact that $(\mathbf{B}|\widetilde{\mathbf{a}^\perp})$ is a basis of $\mathbb{Z}_p^{k+1}$ with probability $1 - 2^{\Omega(-\lambda)}$ over the choices of $\mathbf{B}$ and $\widetilde{\mathbf{a}^\perp}$ (by the basis property in Definition 1). Finally, we use the fact that when $(\mathbf{B}|\widetilde{\mathbf{a}^\perp})$ is a basis of $\mathbb{Z}_p^{k+1}$, the distribution of $(\mathbf{Bs} + \widetilde{s}\widetilde{\mathbf{a}^\perp})$ is $1/p$-close to the distribution of $\mathbf{z} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$.

Moreover, $\mathsf{KeyGenO}(\alpha)$ is simulated by computing $\widehat{K} := [u]_2 \leftarrow_{\mathrm{R}} \mathbb{G}_2$, and $K := [\sum_{i,j}\alpha_{i,j}\big(\mathbf{Ar}_i + x_i^{(b)}\mathbf{b}^\perp\big)^\top\big(\mathbf{Bs}_j + y_j^{(b)}\mathbf{z}\big) - \sum_{i,j}\alpha_{i,j}x_i^{(b)}(\mathbf{b}^\perp)^\top(\mathbf{Bs}_j + y_j^{(b)}\mathbf{z})]_1 - [u]_1$, which does not require to know $[\mathbf{A}]_2$. Then, we switch $\{\mathbf{r}_i\}_{i\in[n]}$ to $\{\mathbf{r}_i + x_i^{(b)}\mathbf{r}\}_{i\in[n]}$, where $\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, which does not change the distribution of the game. So we have, for all $i \in [n]$, $C_i := [\mathbf{Ar}_i + x_i^{(b)}(\mathbf{Ar} + \mathbf{b}^\perp)]_1$. At this point, the game can be simulated knowing $[\mathbf{A}]_1, [\mathbf{Ar}]_1$, and other information completely independent from the latter.

Therefore, we can use the mddh assumption with respect to $[\mathbf{A}]_1$ to argue that:

$$([\mathbf{A}]_1, [\mathbf{Ar}]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{u}]_1) \equiv ([\mathbf{A}]_1, [\mathbf{u}]_1 - [\mathbf{b}^\perp]_1) \approx_c ([\mathbf{A}]_1, [\mathbf{Ar}]_1 - [\mathbf{b}^\perp]_1),$$

where $\mathbf{r} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and $\mathbf{u} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$, $\approx_c$ denotes computational indistinguishability, and $\equiv$ denotes statistical equality. This means for all $i \in [n]$, $C_i := [\mathbf{Ar}_i + x_i^{(b)}\mathbf{Ar}]_1$.

Switching back $\{\mathbf{r}_i + x_i^{(b)}\mathbf{r}\}_{i\in[n]}$ to $\{\mathbf{r}_i\}_{i\in[n]}$, and $\{\mathbf{Bs}_j + y_j(b)\mathbf{z}\}_{j\in[m]}$ back to $\{\mathbf{Bs}_j + y_j^{(b)}\mathbf{a}^\perp\}_{j\in[m]}$, we obtain $C_i := [\mathbf{Ar}_i]_1$, $\widehat{C}_j := [\mathbf{Bs}_j + y_j^{(b)}\mathbf{a}^\perp]_2$, $\widehat{K} := [u]_2 \leftarrow_{\mathrm{R}} \mathbb{G}_2$, and

$$\begin{aligned} K &:= [\sum_{i,j}\alpha_{i,j}\big(\mathbf{Ar}_i\big)^\top\big(\mathbf{Bs}_j + y_j^{(b)}\mathbf{a}^\perp\big) - \sum_{i,j}\alpha_{i,j}x_i^{(b)}(\mathbf{b}^\perp)^\top(\mathbf{Bs}_j + y_j^{(b)}\mathbf{a}^\perp)]_1 - [u]_1 \\ &= [\sum_{i,j}\alpha_{i,j}\big(\mathbf{Ar}_i\big)^\top\mathbf{Bs}_j - (\mathbf{b}^\perp)^\top\mathbf{a}^\perp\sum_{i,j}\alpha_{i,j}x_i^{(b)}y_j^{(b)}]_1 - [u]_1, \end{aligned}$$

which is as in the game G_1. □

Lemma 2 **(G_1 to G_2).** *There exists an adversary $\mathcal{B}_1$ such that $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ and*

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

Proof of Lemma 2. 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 $[\mathbf{B}]_1$.

First, note that the vector $\mathbf{b}^\perp$ only shows up in the value $(\mathbf{b}^\perp)^\top \mathbf{a}^\perp$ used by $\mathsf{KeyGenO}$. Therefore, the adversary $\mathcal{B}_1$ simulates $\mathsf{KeyGenO}$ by picking a uniformly random value $(\mathbf{b}^\perp)^\top \mathbf{a}^\perp \leftarrow_{\mathrm{R}} \mathbb{Z}_p$. In particular, it does not need to know $\mathbf{b}^\perp$ explicitly.

Then, $\mathcal{B}_1$ computes secret keys $K := [u]_1 \leftarrow_{\mathrm{R}} \mathbb{G}_1$, and $\widehat{K} := [\sum_{i,j} \alpha_{i,j} \mathbf{r}_i^\top \mathbf{A}^\top (\mathbf{B}\mathbf{s}_j + y_j^{(b)} \mathbf{a}^\perp)]_2 - [u]_2 - (\mathbf{b}^\perp)^\top \mathbf{a}^\perp \cdot [\sum_{i,j} \alpha_{i,j} x_i^{(b)} y_j^{(b)}]_2$, which is distributed as in G_1, since $\mathbf{A}^\top \mathbf{a}^\perp = \mathbf{0}$.

Then, we argue that $[\mathbf{B}\mathbf{s}_j + y_j^{(b)} \mathbf{a}^\perp]_2$ is statistically close to $[\mathbf{B}\mathbf{s}_j + y_j^{(b)} \mathbf{z}]_2$, where $\mathbf{z} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, as exactly as in the proof of Lemma 1.

Then, we use the mddh with respect to $[\mathbf{B}]_2$ to argue that:

$$([\mathbf{B}]_2, [\mathbf{z}]_2) \approx_c ([\mathbf{B}]_2, [\mathbf{B}\mathbf{s}]_2),$$

where $\mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and $\mathbf{z} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$, and $\approx_c$ denotes computational indistinguishability. For all $j \in [m]$, we obtain $\widehat{C}_j := [\mathbf{B}\mathbf{s}_j + y_j^{(b)} \mathbf{B}\mathbf{s}]_2$ and $\widehat{K} := [\sum_{i,j} \alpha_{i,j} \mathbf{r}_i^\top \mathbf{A}^\top (\mathbf{B}\mathbf{s}_j + y_j^{(b)} \mathbf{B}\mathbf{s})]_2 - [u]_2 - (\mathbf{b}^\perp)^\top \mathbf{a}^\perp \cdot [\sum_{i,j} \alpha_{i,j} x_i^{(b)} y_j^{(b)}]_2$, which is identically distributed as G_2, using the fact that $\{\mathbf{s}_j\}_{j \in [m]}$ is identically distributed than $\{\mathbf{s}_j + y_j^{(b)} \mathbf{s}\}_{j \in [m]}$, when $\mathbf{s}_j, \mathbf{s} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$.

□

Lemma 3 **(G_2).** $\mathsf{Adv}_2 = 0$.

Proof of Lemma 3. By definition of the security game, for all α queried to $\mathsf{KeyGenO}$, we have: $\sum_{i,j} \alpha_{i,j} x_i^{(b)} y_j^{(b)} = \sum_{i,j} \alpha_{i,j} x_i^{(0)} y_j^{(0)}$. Therefore, the view of the adversary in G_2 is completely independent from the random bit $b \leftarrow_{\mathrm{R}} \{0,1\}$. □

Combining Lemma 1, 2, and 3 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 3.2 is selectively secure under the $\mathcal{D}_k$-mddh and the 3-pddh assumptions, on asymmetric pairings.

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 3.2 has perfect correctness.*

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

$$e(C_{2i-1}, \widehat{C}_{2j-1}) = [\gamma \mathbf{r}_{2i-1}^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_{2j-1} + x_i y_j]_T \text{ and } e(C_{2i}, \widehat{C}_{2j}) = [\gamma \mathbf{r}_{2i}^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_{2j}]_T.$$

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

$\underline{\mathsf{KeyGen}(\mathsf{msk}, \alpha \in \mathbb{Z}_p^{n\cdot m})}$:
$K := [\sum_{i\in[n],j\in[m]} \alpha_{i,j}\big(\mathbf{r}_{2i-1}^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_{2j-1} - \mathbf{r}_{2i}^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_{2j}\big)]_1 - [u]_1 \in \mathbb{G}_1$; $\widehat{K} := [u]_2 \in \mathbb{G}_2$, where $u \leftarrow_{\text{R}} \mathbb{Z}_p$.
Return $\mathsf{sk}_\alpha := (K, \widehat{K}) \in \mathbb{G}_1 \times \mathbb{G}_2$

$\underline{\mathsf{Enc}(\mathsf{pk}, (\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^m)}$:
$\mathbf{W} \leftarrow_{\text{R}} \mathsf{GL}_{k+2}$, $\gamma \leftarrow_{\text{R}} \mathbb{Z}_p$; $C_0 := [\gamma]_1$; $\widehat{C}_0 := [\gamma]_2$; for $1 \le i \le n, 1 \le j \le m$:
$C_{2i-1} := \left[\begin{pmatrix}\gamma \cdot \mathbf{A}\mathbf{r}_{2i-1} \\ x_i\end{pmatrix}^\top \mathbf{W}^{-1}\right]_1$, $C_{2i} := \big[\gamma(\mathbf{A}\mathbf{r}_{2i})^\top\big]_1$, $\widehat{C}_{2j-1} := \left[\mathbf{W}\begin{pmatrix}\mathbf{B}\mathbf{s}_{2j-1} \\ y_j\end{pmatrix}\right]_2$ $\widehat{C}_{2j} := [\mathbf{B}\mathbf{s}_{2j}]_2$
Return $\mathsf{ct}_{(\mathbf{x},\mathbf{y})} := \Big(\{C_i, \widehat{C_j}\}_{0\le i\le 2n, 0\le j\le 2m}\Big) \in \mathbb{G}_1^{n(2k+3)+1} \times \mathbb{G}_2^{m(2k+3)+1}$

$\underline{\mathsf{Dec}(\mathsf{pk}, \mathsf{ct}_{(\mathbf{x},\mathbf{y})}, \mathsf{sk}_\alpha)}$:
Return $\sum_{i\in[n],j\in[m]} \alpha_{i,j}\big(e(C_{2i-1}, \widehat{C}_{2j-1}) + e(C_{2i}, \widehat{C}_{2j})\big) - e(C_0, \widehat{K}) - e(K, \widehat{C}_0)$.
```

Fig. 3. $\mathsf{FE}(k, \mathcal{D}_k)$, 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.

Therefore, the decryption gets

$$[\sum_{i\in[n],j\in[m]} \alpha_{i,j}\gamma\big(\mathbf{r}_{2i-1}^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_{2j-1} + \mathbf{r}_{2i}^\top \mathbf{A}^\top \mathbf{B}\mathbf{s}_{2j}\big)]_T + [\sum_{i\in[n],j\in[m]} \alpha_{i,j} x_i y_j]_T - e(C_0, \widehat{K}) - e(K, \widehat{C}_0)$$
$$= [\sum_{i\in[n],j\in[m]} \alpha_{i,j} x_i y_j]_T.$$

□

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 $\mathbb{G}$, then the functional encryption scheme $\mathsf{FE}(k, \mathcal{D}_k)$ defined in Figure 3.2 is selectively secure. Namely, for any adversary $\mathcal{A}$, there exists adversaries $\mathcal{B}$ and $\mathcal{B}'$ such that $\mathbf{T}(\mathcal{B}') \approx \mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A})$ and*

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{FE}}(\lambda) \le 12 \cdot \mathbf{Adv}_{\mathsf{GGen},\mathcal{B}}^{\mathcal{D}_k\text{-}\mathsf{mddh}}(\lambda) + 2 \cdot \mathbf{Adv}_{\mathsf{GGen},\mathcal{B}'}^{3-\mathsf{pddh}}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof of 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

Lemma 4 (G_0 to G_1). *There exists an adversary $\mathcal{B}_0$ such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A})$ and*

$$|\mathsf{Adv}_0 - \mathsf{Adv}_1| \le 6 \cdot \mathbf{Adv}_{\mathsf{GGen},\mathcal{B}_0}^{\mathcal{D}_k\text{-}\mathsf{mddh}}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof of Lemma 4. Using the selective, single-ciphertext security of the underlying private-key scheme (which is exactly the scheme in Figure 3.1), we can switch: $\{[\mathbf{A}\mathbf{r}_i]_1, [\mathbf{B}\mathbf{s}_j]_2\}_{i\in[2n],j\in[2m]}$

```
$\underline{\mathsf{SetupO}\big((\mathbf{x}^{(0)},\mathbf{y}^{(0)}),(\mathbf{x}^{(1)},\mathbf{y}^{(1)})\big)}$:        $\colorbox{lightgray}{$\mathrm{G}_0$}$, $\boxed{\colorbox{lightgray}{$\mathrm{G}_1$}, \bbox[border:1px dashed black]{\colorbox{lightgray}{$\mathrm{G}_2$}, \mathrm{G}_3}, \mathrm{G}_4}$, $\mathrm{G}_5$
$\mathcal{PG} \leftarrow_{\mathrm{R}} \mathsf{GGen}(1^\lambda)$; $\mathbf{A},\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$; $b \leftarrow_{\mathrm{R}} \{0,1\}$; $\boxed{\mathbf{a}^\perp,\mathbf{b}^\perp \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1} \text{ s.t. } \mathbf{A}^\top\mathbf{a}^\perp = \mathbf{B}^\top\mathbf{b}^\perp = \mathbf{0}}$
For $i \in [2n], j \in [2m]$: $\mathbf{r}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$
$\mathsf{pk} := \left\{\left[\mathbf{Ar}_{2i-1} + \boxed{x_i^{(b)}\mathbf{b}^\perp}\right]_1, \left[\mathbf{Ar}_{2i} + \boxed{x_i^{(0)}\mathbf{b}^\perp}\right]_1, \left[\mathbf{Bs}_{2j-1} + \boxed{y_j^{(b)}\mathbf{a}^\perp}\right]_2, \left[\mathbf{Bs}_{2j} + \boxed{y_j^{(0)}\mathbf{a}^\perp}\right]_2\right\}_{i\in[n],j\in[m]}$
$\mathbf{W} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$, $\gamma \leftarrow_{\mathrm{R}} \mathbb{Z}_p$; $\bbox[border:1px dashed black]{v \leftarrow_{\mathrm{R}} \mathbb{Z}_p}$; $C_0 := [\gamma]_1$; $\widehat{C}_0 := [\gamma]_2$
$C_{2i-1} := \left[\begin{pmatrix} \gamma\mathbf{Ar}_{2i-1} + \boxed{\gamma x_i^{(b)}\mathbf{b}^\perp} + \bbox[border:1px dashed black]{v x_i^{(b)}\mathbf{b}^\perp} \\ 0 + \colorbox{lightgray}{$x_i^{(b)}$} \end{pmatrix}^\top \mathbf{W}^{-1}\right]_1$;   $C_{2i} := \left[\left(\gamma\mathbf{Ar}_{2i} + \boxed{\gamma x_i^{(0)}\mathbf{b}^\perp} + \bbox[border:1px dashed black]{v x_i^{(0)}\mathbf{b}^\perp}\right)^\top\right]_1$;
$\widehat{C}_{2j-1} := \left[\mathbf{W}\begin{pmatrix} \mathbf{Bs}_{2j-1} + \boxed{y_j^{(b)}\mathbf{b}^\perp} \\ 0 + \colorbox{lightgray}{$y_j^{(b)}$} \end{pmatrix}\right]_2$; $\widehat{C}_{2j} := \left[\mathbf{Bs}_{2j} + \boxed{y_j^{(0)}\mathbf{b}^\perp}\right]_2$;
Return $(\mathsf{pk}, \mathsf{ct}_{(\mathbf{x},\mathbf{y})} := \{C_i, \widehat{C_j}\}_{0\le i\le 2n, 0\le j\le 2m})$

$\underline{\mathsf{KeyGenO}(\alpha \in \mathbb{Z}_p^{n\cdot m})}$:
$K := [\sum_{i\in[n],j\in[m]} \alpha_{i,j}\big(\mathbf{r}_{2i-1}^\top\mathbf{A}^\top\mathbf{Bs}_{2j-1} + \mathbf{r}_{2i}^\top\mathbf{A}^\top\mathbf{Bs}_{2j}\big)]_1 - [u]_1 \in \mathbb{G}_1$; $\widehat{K} := [u]_2 \in \mathbb{G}_2$, where $u \leftarrow_{\mathrm{R}} \mathbb{Z}_p$.
Return $\mathsf{sk}_\alpha := (K, \widehat{K}) \in \mathbb{G}_1 \times \mathbb{G}_2$
```

Fig. 4. Games G_i, $i = 0,\ldots,5$ for the proof of selective security of $\mathsf{FE}(k,\mathcal{D}_k)$ in Figure 3.2. In each procedure, the components inside a solid (dotted, light gray, gray) frame are only present in the games marked by a solid (dotted, light gray, gray) frame.

to $\{[\mathbf{Ar}_{2i-1} + x_i^{(b)}\mathbf{b}^\perp]_1, [\mathbf{Ar}_{2i} + x_i^{(0)}\mathbf{b}^\perp]_1, [\mathbf{Bs}_{2j-1} + y_j^{(b)}\mathbf{a}^\perp]_2, [\mathbf{Bs}_{2j} + y_j^{(0)}\mathbf{a}^\perp]_2\}_{i\in[n],j\in[m]}\}$, since $\sum_{i\in[n],j\in[m]} \alpha_{i,j}x_i^{(b)}y_j^{(b)} - \sum_{i\in[n],j\in[m]} \alpha_{i,j}x_i^{(0)}y_j^{(0)} = 0$, by definition of the security game. Thus, by Theorem 2 (security of the single-ciphertext secure scheme), we obtain the lemma. □

Lemma 5 (G_1 to G_2). *There exists an adversary $\mathcal{B}_1$ such that $\mathbf{T}(\mathcal{B}_1) \approx \mathbf{T}(\mathcal{A})$ and*

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

Here, we change the distribution of the challenge ciphertexts, first using the 3-pddh assumption. *Proof of Lemma 5.* Upon receiving a 3-pddh challenge $(\mathcal{PG}, [a]_1, [b]_2, [c]_1, [c]_2, [z]_1)$ (see Definition 3), $\mathcal{B}_1$ simulates $\mathsf{SetupO}((\mathbf{x}^{(0)},\mathbf{y}^{(0)}),(\mathbf{x}^{(1)},\mathbf{y}^{(1)}))$ by picking $\mathbf{A},\mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$; $b \leftarrow_{\mathrm{R}} \{0,1\}$; $\widetilde{\mathbf{b}}^\perp \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ s.t. $\mathbf{B}^\top\widetilde{\mathbf{b}}^\perp = \mathbf{0}$; $\widetilde{\mathbf{a}}^\perp \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ s.t. $\mathbf{A}^\top\widetilde{\mathbf{a}}^\perp = \mathbf{0}$, $(\widetilde{\mathbf{a}}^\perp)^\top\widetilde{\mathbf{b}}^\perp = 1$, and setting:

$$[\mathbf{a}^\perp]_2 := [b \cdot \widetilde{\mathbf{a}}^\perp]_2, [\mathbf{b}^\perp]_1 := [a \cdot \widetilde{\mathbf{b}}^\perp]_1 \text{ and } \gamma := c.$$

Then, for $i \in [2n], j \in [2m]$, $\mathcal{B}_1$ picks $\mathbf{r}_i \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$, $\mathbf{s}_j \leftarrow_{\mathrm{R}} \mathbb{Z}_p^k$ and computes

$$\mathsf{pk} := \left\{\left[\mathbf{Ar}_{2i-1} + x_i^{(b)}\mathbf{b}^\perp\right]_1, \left[\mathbf{Ar}_{2i} + x_i^{(0)}\mathbf{b}^\perp\right]_1, \left[\mathbf{Bs}_{2j-1} + y_j^{(b)}\mathbf{a}^\perp\right]_2, \left[\mathbf{Bs}_{2j} + y_j^{(0)}\mathbf{a}^\perp\right]_2\right\}_{i\in[n],j\in[m]}.$$

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

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

Here we use the fact that $(\mathbf{B}|\mathbf{a}^{\perp})$ is full rank with probability $1-2^{-\Omega(\lambda)}$ over the choices of $\mathbf{B}$ and $\mathbf{a}^{\perp}$ (see Definition 1). Then, for $i \in [n], j \in [m]$, it computes

$$C_{2i-1} := \left[\begin{pmatrix} \gamma \mathbf{r}_{2i-1} \\ z \cdot x_i^{(b)} \\ x_i^{(b)} \end{pmatrix}^{\top} \left(\begin{array}{c|c|c} \mathbf{A}^{\top}\mathbf{B} & 0 & 0 \\ \hline 0 & \underbrace{(\widetilde{\mathbf{b}}^{\perp})^{\top}\widetilde{\mathbf{a}}^{\perp}}_{=1} & 0 \\ \hline 0 & 0 & 1 \end{array} \right) \widetilde{\mathbf{W}}^{-1} \right]_1 \text{ and } C_{2i} := \left[\begin{pmatrix} \gamma \mathbf{r}_{2i} \\ z \cdot x_i^{(0)} \\ 0 \end{pmatrix}^{\top} \left(\begin{array}{c|c|c} \mathbf{A}^{\top}\mathbf{B} & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array} \right) \widetilde{\mathbf{W}}^{-1} \right]_1$$

$$\widehat{C}_{2j-1} := \left[\widetilde{\mathbf{W}} \begin{pmatrix} \mathbf{s}_{2j-1} \\ y_j^{(b)} \\ y_j^{(b)} \end{pmatrix} \right]_2 \text{ and } \widehat{C}_{2j} := \left[\widetilde{\mathbf{W}} \begin{pmatrix} \mathbf{s}_{2j} \\ y_j^{(0)} \\ 0 \end{pmatrix} \right]_2$$

Finally, $\mathcal{B}_1$ computes $C_0 := [c]_1$, $\widehat{C}_0 := [c]_2$, and simulates $\mathsf{KeyGenO}$ as in G_2 (see Figure 3.2). Note that when $[z]_1$ is a real 3-pddh challenge, i.e $[z]_1 = [abc]_1$, then $\mathcal{B}_1$ simulates G_1; whereas it simulates G_2 when $[z]_1 := [v]_1 \leftarrow_{\mathrm{R}} \mathbb{G}_1$. This proves $|\mathsf{Adv}_1 - \mathsf{Adv}_2| \leq \mathbf{Adv}^{3-\mathsf{pddh}}_{\mathsf{GGen},\mathcal{B}_1}(\lambda) + 2^{-\Omega(\lambda)}$. □

Lemma 6 **(G_2 to G_3).** $|\mathsf{Adv}_2 - \mathsf{Adv}_3| \leq 2^{-\Omega(\lambda)}$.

Here, we change the distribution of the challenge ciphertexts, using a statistical argument.
Proof of Lemma 6. We use the facts that:

- the distributions of $v \leftarrow_{\mathrm{R}} \mathbb{Z}_p$, and $v \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ such that $v + \gamma \neq 0$, have statistical distance $1/p$, for any $\gamma \in \mathbb{Z}_p$.
- $\mathbf{W} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$ and $\widetilde{\mathbf{W}} \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k \times k} & 0 & 0 \\ \hline 0 & 1 & \frac{1}{v+\gamma} \\ \hline 0 & 0 & \frac{-1}{v+\gamma} \end{array} \right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k \times k} & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & -1 & 1 \end{array} \right) \cdot \left(\begin{array}{c|c} \mathbf{B}|\mathbf{a}^{\perp} & 0 \\ \hline \mathbf{0} & 1 \end{array} \right)^{-1}$, where $\widetilde{\mathbf{W}} \leftarrow_{\mathrm{R}} \mathsf{GL}_{k+2}$ and $v \leftarrow_{\mathrm{R}} \mathbb{Z}_p, v + \gamma \neq 0$, are statistically $2^{-\Omega(\lambda)}$-close, since $(\mathbf{B}|\mathbf{a}^{\perp})$ forms a basis of $\mathbb{Z}_p^{k+1}$ with probability $1 - 2^{-\Omega(\lambda)}$ over the choice of $\mathbf{B}$ and $\mathbf{a}^{\perp}$.

Therefore, we can change the distribution of C_i and $\widehat{C}_j$, for all $i \in [n], j \in [m]$, as follows:

$$\begin{aligned} \widehat{C}_{2j-1} &= \left[\widetilde{\mathbf{W}} \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k \times k} & 0 & 0 \\ \hline 0 & 1 & \frac{1}{v+\gamma} \\ \hline 0 & 0 & \frac{-1}{v+\gamma} \end{array} \right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k \times k} & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & -1 & 1 \end{array} \right) \begin{pmatrix} \mathbf{s}_{2j-1} \\ y_j^{(b)} \\ y_j^{(b)} \end{pmatrix} \right]_2 \\ &= \left[\widetilde{\mathbf{W}} \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k \times k} & 0 & 0 \\ \hline 0 & 1 & \frac{1}{v+\gamma} \\ \hline 0 & 0 & \frac{-1}{v+\gamma} \end{array} \right) \begin{pmatrix} \mathbf{s}_{2j-1} \\ y_j^{(b)} \\ 0 \end{pmatrix} \right]_2 \\ &= \left[\widetilde{\mathbf{W}} \cdot \begin{pmatrix} \mathbf{s}_{2j-1} \\ y_j^{(b)} \\ 0 \end{pmatrix} \right]_2 \end{aligned}$$

and

$$
\begin{aligned}
C_{2i-1} &= \left[\begin{pmatrix} \gamma \mathbf{r}_{2i-1} \\ (v+\gamma) \cdot x_i^{(b)} \\ x_i^{(b)} \end{pmatrix}^{\top} \left(\begin{array}{c|c|c} \mathbf{A}^{\top}\mathbf{B} & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & -1 & 1 \end{array}\right)^{-1} \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & 1 & \frac{1}{v+\gamma} \\ \hline 0 & 0 & \frac{-1}{v+\gamma} \end{array}\right)^{-1} \cdot \widetilde{\mathbf{W}}^{-1} \right]_1 \\
&= \left[\begin{pmatrix} \gamma \mathbf{r}_{2i-1} \\ (v+\gamma) \cdot x_i^{(b)} \\ x_i^{(b)} \end{pmatrix}^{\top} \left(\begin{array}{c|c|c} \mathbf{A}^{\top}\mathbf{B} & 0 & 0 \\ \hline 0 & 1 & 0 \\ \hline 0 & 1 & 1 \end{array}\right) \cdot \left(\begin{array}{c|c|c} \mathsf{Id}_{k\times k} & 0 & 0 \\ \hline 0 & 1 & \frac{1}{v+\gamma} \\ \hline 0 & 0 & \frac{-1}{v+\gamma} \end{array}\right)^{-1} \cdot \widetilde{\mathbf{W}}^{-1} \right]_1 \\
&= \left[\begin{pmatrix} \gamma \mathbf{r}_{2i-1} \\ (v+\gamma) \cdot x_i^{(b)} \\ x_i^{(b)} \end{pmatrix}^{\top} \left(\begin{array}{c|c|c} \mathbf{A}^{\top}\mathbf{B} & 0 & 0 \\ \hline 0 & 1 & 1 \\ \hline 0 & 1 & -(v+\gamma) \end{array}\right) \cdot \widetilde{\mathbf{W}}^{-1} \right]_1 \\
&= \left[\begin{pmatrix} \gamma \mathbf{r}_{2i-1} \\ (v+\gamma+1) \cdot x_i^{(b)} \\ 0 \end{pmatrix}^{\top} \cdot \widetilde{\mathbf{W}}^{-1} \right]_1
\end{aligned}
$$

Finally, we can switch $\{v+\gamma+1, \text{ where } v \leftarrow_{\mathrm{R}} \mathbb{Z}_p \text{ such that } v+\gamma \neq 0\}$, to $\{v+\gamma, \text{ where } v \leftarrow_{\mathrm{R}} \mathbb{Z}_p\}$, because these distributions are $1/p$ close, to obtain the distribution of G_3. This proves $|\mathsf{Adv}_2 - \mathsf{Adv}_3| \leq 2^{-\Omega(\lambda)}$. □

Lemma 7 (G_3 to G_4). *There exists an adversary $\mathcal{B}_3$ such that $\mathbf{T}(\mathcal{B}_3) \approx \mathbf{T}(\mathcal{A})$ and*

$$|\mathsf{Adv}_3 - \mathsf{Adv}_4| \leq \mathbf{Adv}^{3-\mathsf{pddh}}_{\mathsf{GGen},\mathcal{B}_2}(\lambda).$$

Here, we change the distribution of the challenge ciphertext, using the 3-pddh assumption, as for Lemma 6.

Proof of Lemma 7. Upon receiving a 3-pddh challenge $(\mathcal{PG}, [a]_1, [b]_2, [c]_1, [c]_2, [z]_1)$, $\mathcal{B}_3$ simulates $\mathsf{SetupO}((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), (\mathbf{x}^{(1)}, \mathbf{y}^{(1)}))$ by picking $\mathbf{A}, \mathbf{B} \leftarrow_{\mathrm{R}} \mathcal{D}_k$; $b \leftarrow_{\mathrm{R}} \{0,1\}$; $\widetilde{\mathbf{b}}^{\perp} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ s.t. $\mathbf{B}^{\top}\widetilde{\mathbf{b}}^{\perp} = \mathbf{0}$; $\widetilde{\mathbf{a}}^{\perp} \leftarrow_{\mathrm{R}} \mathbb{Z}_p^{k+1}$ s.t. $\mathbf{A}^{\top}\widetilde{\mathbf{a}}^{\perp} = \mathbf{0}$, $(\widetilde{\mathbf{a}}^{\perp})^{\top}\widetilde{\mathbf{b}}^{\perp} = 1$, and setting:

$$[\mathbf{a}^{\perp}]_2 := [b \cdot \widetilde{\mathbf{a}}^{\perp}]_2, [\mathbf{b}^{\perp}]_1 := [a \cdot \widetilde{\mathbf{b}}^{\perp}]_1 \text{ and } \gamma := c.$$

The proof goes on exactly as for the proof of Lemma 5, to which we defer for further details. □

Lemma 8 (G_4 to G_5). *There exists an adversary $\mathcal{B}_4$ such that $\mathbf{T}(\mathcal{B}_4) \approx \mathbf{T}(\mathcal{A})$ and*

$$|\mathsf{Adv}_4 - \mathsf{Adv}_5| \leq 4 \cdot \mathbf{Adv}^{\mathcal{D}_k\text{-}\mathsf{mddh}}_{\mathsf{GGen},\mathcal{B}_4}(\lambda) + 2^{-\Omega(\lambda)}.$$

Proof of Lemma 8. This transition is symmetric to that between G_0 and G_1: we use the selective, single-ciphertext security of the underlying private-key scheme (in Figure 3.1), to switch: $\{[\mathbf{A}\mathbf{r}_{2i-1} + x_i^{(b)}\mathbf{b}^{\perp}]_1, [\mathbf{A}\mathbf{r}_{2i} - x_i^{(0)}\mathbf{b}^{\perp}]_1, [\mathbf{B}\mathbf{s}_{2j-1} + y_j^{(b)}\mathbf{a}^{\perp}]_2, [\mathbf{B}\mathbf{s}_{2j} + y_j^{(0)}\mathbf{a}^{\perp}]_2\}_{i\in[n],j\in[m]}$ to $\{[\mathbf{A}\mathbf{r}_i]_1, [\mathbf{B}\mathbf{s}_j]_2\}_{i\in[2n],j\in[2m]}$, since $\sum_{i\in[n],j\in[m]} \alpha_{i,j} x_i^{(b)} y_j^{(b)} + \sum_{i\in[n],j\in[m]} \alpha_{i,j} x_i^{(0)} y_j^{(0)} = 0$, 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 4-8, and the fact that 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 build a PE for degree-two polynomial evaluation, namely, for the predicate $\mathsf{P} : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ where $\mathcal{X} \subset \mathbb{Z}_p^n \times \mathbb{Z}_p^m$, $\mathcal{Y} \subset \mathbb{Z}_p^{n \cdot m}$, such that and for all $(x, y) \in \mathcal{X}$ and $\alpha \in \mathcal{Y}$,

$$\sum_{i \in [n], j \in [m]} \alpha_{i,j} x_i y_j \in \{0,1\} \text{ and } \mathsf{P}((\mathbf{x},\mathbf{y}),\alpha) = 1 \text{ iff } \sum_{i \in [n], j \in [m]} \alpha_{i,j} x_i y_j = 1 \mod p.$$

In Figure 4, we present a generic construction of PE for P from any functional encryption scheme FE for quadratic functions, namely, for $F : \mathcal{X}' \times \mathcal{K} \to \mathcal{Y}'$ where $\mathcal{X}' \subset \mathbb{Z}_p^n \times \mathbb{Z}_p^m$, $\mathcal{K} \subset \mathbb{Z}_p^{n \cdot m}$, $\mathcal{Y}' := F(\mathcal{X}', \mathcal{K})$ and for all $(\mathbf{x},\mathbf{y}) \in \mathcal{X}'$, $\alpha \in \mathcal{K}$

$$F((\mathbf{x},\mathbf{y}),\alpha) = \left[\sum_{i \in [n], j \in [m]} \alpha_{i,j} x_i y_j \right]_T .$$

Such functional encryption scheme is given in Section 3.

```
$\underline{\mathsf{Setup}(1^\lambda, \mathcal{X} \subset \mathbb{Z}_p^n \times \mathbb{Z}_p^m, \mathcal{Y} \subset \mathbb{Z}_p^{n \cdot m}, 1^k, \mathcal{M} := \mathbb{G}_T, \mathcal{D}_k):}$
Set $\mathcal{X}' := \{(w \cdot \mathbf{x}, \mathbf{y}), (\mathbf{x},\mathbf{y}) \in \mathcal{X}, w \in \mathbb{Z}_p\}$
$\mathcal{K} := \mathcal{Y}$, and $\mathcal{Y}' := \mathbb{Z}_p$.
Return $(\mathsf{pk}, \mathsf{msk}) \leftarrow_{\mathrm{R}} \mathsf{Setup}_{\mathsf{FE}}(1^\lambda, \mathcal{X}', \mathcal{K}, \mathcal{Y}', 1^k, \mathcal{D}_k, )$

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

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

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

Fig. 5. $\mathsf{PE}(k, \mathcal{D}_k)$, a family of functional encryption schemes parametrized by $k \in \mathbb{N}^*$ and a matrix distribution $\mathcal{D}_k$, selectively secure 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). *Let $k \in \mathbb{N}^*$ and $\mathcal{D}_k$ be a matrix distribution. Let* $\mathsf{FE} := (\mathsf{Setup}_{\mathsf{FE}}, \mathsf{KeyGen}_{\mathsf{FE}}, \mathsf{Enc}_{\mathsf{FE}}, \mathsf{Dec}_{\mathsf{FE}})$ *be a functional encryption scheme for $F : \mathcal{X}' \times \mathcal{K} \to \mathcal{Y}'$ where for all $(\mathbf{x},\mathbf{y}) \in \mathcal{X}'$, $\alpha \in \mathcal{K}$, $F((\mathbf{x},\mathbf{y}),\alpha) = \left[\sum_{i,j \in [n]} \alpha_{i,j} x_i y_j\right]_T$. If* FE *is perfectly correct, then, so is the attribute-based encryption scheme* $\mathsf{PE}(k, \mathcal{D}_k)$ *defined in Figure 4.*

Proof of Theorem 5. By correctness of FE, we have for all $(\mathbf{x},\mathbf{y}) \in \mathcal{X}$, $w \in \mathbb{Z}_p$, $\alpha \in \mathcal{Y}$: $(w\mathbf{x},\mathbf{y}) \in \mathcal{X}'$, $\alpha \in \mathcal{K}'$, and

$$F((w \cdot \mathbf{x},\mathbf{y}),\alpha) = \left[w \cdot \sum_{i \in [n], j \in [m]} \alpha_{i,j} x_i y_j \right] = [w \cdot \mathsf{P}((\mathbf{x},\mathbf{y}),\alpha)]_T .$$

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

Theorem 6 (Security). *Let $k \in \mathbb{N}^*$ and $\mathcal{D}_k$ be a matrix distribution. Let* $\mathsf{FE} := (\mathsf{Setup}_{\mathsf{FE}}, \mathsf{KeyGen}_{\mathsf{FE}}, \mathsf{Enc}_{\mathsf{FE}}, \mathsf{Dec}_{\mathsf{FE}})$ *be a functional encryption scheme for $F : \mathcal{X}' \times \mathcal{K} \to \mathcal{Y}'$ where for all $(\mathbf{x},\mathbf{y}) \in \mathcal{X}'$, $\alpha \in \mathcal{K}$, $F((\mathbf{x},\mathbf{y}),\alpha) = \left[\sum_{i,j \in [n]} \alpha_{i,j} x_i y_j\right]_T$. If* FE *is selectively secure, then, so is the attribute-based encryption scheme* $\mathsf{PE}(k, \mathcal{D}_k)$ *defined in Figure 4.*

Proof of Theorem 6. Let $\mathcal{A}$ be an adversary against the selective security of FE. We build and adversary $\mathcal{B}$ against the selective security of PE such that $\mathbf{T}(\mathcal{B}) \approx \mathbf{T}(\mathcal{A})$ and

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

It is clear that $\mathcal{B}$ can simulate the SetupO and $\mathsf{KeyGenO}$ oracles for the security game of PE from the oracles for the security game of FE. By definition of the security for PE, $\mathcal{A}$ submits $(\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), (\mathbf{x}^{(1)}, \mathbf{y}^{(1)}) \in \mathcal{X}$, $M_0, M_1 \in \mathcal{M}$ such that for all queried sk_α, $\mathsf{P}((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), \alpha) = \mathsf{P}((\mathbf{x}^{(1)}, \mathbf{y}^{(1)}), \alpha)$. This implies that for all $w \in \mathbb{Z}_p$, $F((w \cdot \mathbf{x}^{(0)}, \mathbf{y}^{(0)}), \alpha) = F((w \cdot \mathbf{x}^{(1)}, \mathbf{y}^{(1)}), \alpha)$. Therefore, by security of FE, we can switch the challenge ciphertext $([w]_T + M_b, \mathsf{Enc}_{\mathsf{FE}}(\mathsf{pk}, (w \cdot \mathbf{x}^{(b)}, \mathbf{y}^{(b)})))$ where $b \leftarrow_{\mathrm{R}} \{0,1\}$ to $([w]_T + M_b, \mathsf{Enc}_{\mathsf{FE}}(\mathsf{pk}, (w \cdot \mathbf{x}^{(0)}, \mathbf{y}^{(0)})))$. If have $\mathsf{P}((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), \alpha) = 0$, then we can change it to $([w]_T + M_b, \mathsf{Enc}_{\mathsf{FE}}(\mathsf{pk}, (\mathbf{0}, \mathbf{0})))$, by security of FE, which is independent from the bit b, since M_b is completely masked by the one-time pad $[w]_T$. If $\mathsf{P}((\mathbf{x}^{(0)}, \mathbf{y}^{(0)}), \alpha) = 1$, then, by definition of the security of PE, $M_0 = M_1$ and the challenge ciphertext is independent of b. □

PE for boolean functions. We can use PE in Figure 4 to handle boolean functions of constant degree d in n variables, with ciphertext of $O(n^{d/2})$ group elements, compared to $O(n^d)$ group elements in [24] (the asymptotic is taken for large n, constant d). Note that boolean expressions can be arithmetized into a polynomial that evaluates to 0 or 1, à la [31]. Namely, for boolean variable $x, y \in \{0,1\}$, $\mathsf{AND}(x,y)$ is encoded as $x \cdot y$, $\mathsf{OR}(x,y)$ is encoded as $x + y - x \cdot y$, and $\mathsf{NOT}(x) = 1 - x$.

PE for comparison. We reduce the predicate $\mathsf{P}_{\leq} : [N] \times [N] \to \{0,1\}$ defined for all $x, y \in [N]$ by

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

to a polynomial of degree two, as in [9]. First, any $x \in [N]$ 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 $\mathbf{a} := \begin{pmatrix} \mathbf{1}^{x_1 - 1} \\ \mathbf{0}^{\sqrt{N} - x_1 + 1} \end{pmatrix} \in \{0,1\}^{\sqrt{N}}$ where $\mathbf{1}^\ell$, $\mathbf{0}^\ell$ denote the all-one and all-zero vectors in $\{0,1\}^\ell$, respectively; and $\mathbf{b} := \mathbf{e}_i \in \{0,1\}^{\sqrt{N}}$, where $\mathbf{e}_i$ denotes the i'th vector of the canonical basis of $\mathbb{Z}_p^{\sqrt{N}}$. Finally, $x_2 \in [\sqrt{N}]$ is mapped to $\mathbf{c} := \begin{pmatrix} \mathbf{1}^{x_2} \\ \mathbf{0}^{\sqrt{N} - x_2} \end{pmatrix}$. For all $(x_1, x_2), (y_1, y_2) \in [\sqrt{N}] \times [\sqrt{N}]$:

$$\mathsf{P}_{\leq}((x_1, x_2), (y_1, y_2)) = 1 \text{ iff } \mathbf{a}_{y_1} + \mathbf{b}_{y_1} \cdot \mathbf{c}_{y_2} = 1.$$

This gives a PE for comparison with ciphertexts of $O(\sqrt{N})$ group elements, as in [9, 20]. Namely, using the scheme presented in Figure 3.2, we obtain a PE for comparison with ciphertext size $11\sqrt{N} \cdot |\mathbb{G}_1| + 6\sqrt{N} \cdot |\mathbb{G}_2|$ and secret-key size $|\mathbb{G}_1| + |\mathbb{G}_2|$, compared to ciphertext size $5\sqrt{N} \cdot |\mathbb{G}_1| + 4\sqrt{N} \cdot |\mathbb{G}_2| + |\mathbb{G}_T|$ and secret-key size $|\mathbb{G}_2|$ for [20], 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.
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.
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.
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.
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`.
6. N. Attrapadung, G. Hanaoka, and S. Yamada. A framework for identity-based encryption with almost tight security. LNCS, pages 521–549. Springer, Dec. 2015.
7. N. Bitansky and V. Vaikuntanathan. Indistinguishability obfuscation from functional encryption. In *56th FOCS*, pages 171–190. IEEE Computer Society Press, 2015.
8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. 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.
16. 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.
17. P. Datta, R. Dutta, and S. Mukhopadhyay. Functional encryption for inner product with full function privacy. LNCS, pages 164–195. Springer, 2016.
18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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.
24. 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.

25. 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.
26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. A. Shamir. IP=PSPACE. In *31st FOCS*, pages 11–15. IEEE Computer Society Press, Oct. 1990.
32. 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.
33. 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.
34. 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.
35. H. Wee. Déjà Q: Encore! Un petit IBE. LNCS, pages 237–258. Springer, 2016.