Master project

Blackbox separation of TDFs and PKEs

Max Duparc

Supervised by:

Pr. Serge Vaudenay
and Loïs Huguenin-Dumittan

in LASEC

January 6, 2023

Introduction

ABSTRACT:
We expend on [GMR01] by writing a detailed proof of its separation result which was not provided in the original paper. More precisely, we prove that there are no blackbox reduction from poly-to-one trapdoor functions to semantically secure public key encryption scheme.

In the seminal paper [DH76] where Diffie and Hellman introduced the notion of *public key encryption*, they explained it through the lenses of (what are called) *one-way functions*. Indeed the discrete log problem is the stereotypical one-way problem as given x, computing g^x is easy while the converse is "hard". Their idea for public key encryption was thus to use these *one-way functions* to encrypt messages in order to get ciphertexts that could not be easily reversed. To decipher, theses functions need to have a trapdoor such that, given their trapdoor key, we could easily get back the original message. Therefore, at the beginning, *public key encryption* was seen through the lences of *trapdoor functions*.

Since then, the field of public key encryption has expanded, both in depth and complexity. Many improvements have been introduced and among them the notion of *indistinguishability* [GM82]. It occurs that to be indistinguishable, a *public key encryption* scheme could not use a deterministic encryption algorithm. But this is unlike *trapdoor functions*. This induces an interesting question: Are theses notions "comparable" ?

The short answer is no! This result was proved by Yael GERTNER, Tal MALKIN and Omer REINGOLD and the intuition of the proof was given by the authors in the extended abstract [GMR01]. More precisely, they showed that there exists no blackbox transformation from *trapdoor functions* to *semantically secure public key encryption*.

The goal of this paper is to expend on their original work by providing a detailed proof of their result. To do so, we have decomposed this paper as follows:

- Section 1 focuses on background notions. We will especially focus on the notions of cryptographic primitives and reductions between those primitives.
- Section 2 details the objects that are required in order to prove the separation.
- Section 3 and 4 are dedicated on proving two needed results.

Contents

1 Primitives & Reductions

As our goal is to show the impossibility of black-box reduction between TDFs and PKEs, we first have to provide the necessary definitions and some background before jumping into our problem, which is the goal of the following chapters.

1.1 Cryptographic primitives

Before giving a solid definition of the notion of cryptographic primitive, let's explain the intuition that lies behind it. Hash functions are a common tool in cryptography, so common in fact that there are many different one based on many different mathematical principles. But at the end of the day, we are only interested in the fact that all those are one-way functions and here lies the notion of primitive.
The goal of a primitive is to describe the property of a system, independently of its implementation. To do so, it is defined as such

Definition 1.1 (Cryptographic primitives).
*A **cryptographic primitive** $\mathcal{P}$ is defined as the triple $\big(\mathsf{C}, \mathsf{R}, \mathsf{S}\big)$ with:*

- *The components C: the list of variables. We ask that the first variable is a number (say n), called the **security parameter**. The others can be numbers, sets, functions, relations and polytime (relative to n) probabilistic Turing machines (noted PPT) .*
- *The relations R: the list of logical formulas describing our variables.*
- *The security requirements S: the list of adversarial requirements on our variables. It is important to say that all adversary muss have oracle access to the variables.*[1]

Let's give a view examples, but beforehand, we remind ourselves of the mathematical notion of negligability.

Definition 1.2 (negligible).

$$\mathsf{negl}(\mathsf{n}) = \frac{1}{\omega\big(\mathsf{poly}(\mathsf{n})\big)} = \mathsf{n}^{-\omega(1)}$$

[1] It is done to ensure that the security of the primitive does not come from secrecy.

Example 1.3 (Hash).
The primitive for ***hash functions*** Hash *is defined as follows:*

- $\mathsf{C_{Hash}} = \left[\mathsf{n}, \mathsf{m}, \mathsf{H}\right]$
- $\mathsf{R_{Hash}}$*:*
  1. H *is polytime with respect to* n.
  2. $\mathsf{H(m)} \to \mathsf{h}$ *with* $\mathsf{m} \in \{0,1\}^{\mathsf{n}}, \mathsf{h} \in \{0,1\}^{\mathsf{m}}$.
- $\mathsf{S_{Hash}}$*:*
  1. ***Pre-image resistance****:* $\forall \mathsf{A}\ \mathsf{PPT(n)}$

$$\Pr\left[\mathsf{A}^{\mathsf{C_{Hash}}}(\mathsf{h}) \to \mathsf{x}' \text{ s.t. } \mathsf{H}(\mathsf{x}') = \mathsf{h} \;\middle|\; \mathsf{h} = \mathsf{H}(\mathsf{x}), \mathsf{x} \in_{\$} \{0,1\}^{\mathsf{n}}\right] \leqslant \mathsf{negl(n)}$$

  2. ***Second pre-image resistance****:* $\forall \mathsf{B}\ \mathsf{PPT(n)}$

$$\Pr\left[\mathsf{B}^{\mathsf{C_{Hash}}}(\mathsf{m_1}) \to \mathsf{m_2} \text{ s.t. } \mathsf{H}(\mathsf{m_2}) = \mathsf{H}(\mathsf{m_1}) \;\middle|\; \mathsf{m_1} \in_{\$} \{0,1\}^{\mathsf{n}}\right] \leqslant \mathsf{negl(n)}$$

Note that H *is a deterministic polytime TM.*

Example 1.4 (TDF).
The primitive for ***trapdoor functions*** TDF *is defined as follows:*

- $\mathsf{C_{TDF}} = \left[\lambda, \mathsf{n}, \mathsf{KG}, \mathsf{F}, \mathsf{T}\right]$
- $\mathsf{R_{TDF}}$*:*
  1. $n = \mathsf{poly}(\lambda)$
  2. $\mathsf{KG}, \mathsf{F}, \mathsf{T}$ *are polytime with respect to* λ.
  3. $\mathsf{KG}(1^\lambda) \xrightarrow{\$} (\mathsf{k}, \mathsf{tk})$
  4. $\mathsf{F}(\mathsf{k}, \mathsf{x}) \to \mathsf{u}$ *with* $\mathsf{x} \in \{0,1\}^{\mathsf{n}}$.
  5. $\mathsf{T}(\mathsf{tk}, \mathsf{u}) \to \mathsf{x}$ *or* $\perp$ *with* $\mathsf{x} \in \{0,1\}^{\mathsf{n}}$.
  6. ***Correctness****: Given* $\mathsf{KG}(1^\lambda) \xrightarrow{\$} (\mathsf{k}, \mathsf{tk})$*,* $\forall \mathsf{x} \in \{0,1\}^{\mathsf{n}}$*,* $\mathsf{T}\big(\mathsf{tk}, \mathsf{F}(\mathsf{k}, \mathsf{x})\big) = \mathsf{x}$

- $\mathsf{S}_{\mathsf{TDF}}$*:*

  1. ***One-wayness:*** $\forall \mathsf{A}$ $\mathsf{PPT}(\lambda)$

$$\mathsf{Adv}(\mathsf{A}^{\mathsf{C}}) := \Pr\left[\mathsf{A}^{\mathsf{C}_{\mathsf{TDF}}}(\mathsf{k},\mathsf{u}) \to \mathsf{x} \;\middle|\; \mathsf{KG}(1^{\lambda}) \xrightarrow{\$} (\mathsf{k},\mathsf{tk}),\ \mathsf{x} \in_{\$} \{0,1\}^{\mathsf{n}},\ \mathsf{u} = \mathsf{F}(\mathsf{k},\mathsf{x})\right] \leqslant \mathsf{negl}(\lambda)$$

Note that in this definition, F *and* T *are deterministic polytime TM.*

Example 1.5 (PKE)**.**
The primitive for ***semantically secure public key encryption*** PKE *is defined as follows :*

- $\mathsf{C}_{\mathsf{PKE}} = \left[\lambda, \mathsf{n}, \mathsf{w}, \mathsf{Gen}, \mathsf{E}, \mathsf{D}\right]$
- $\mathsf{R}_{\mathsf{PKE}}$ *is composed of the following requirements:*
  1. n, w *are* $\mathsf{poly}(\lambda)$.
  2. $\mathsf{Gen}, \mathsf{E}, \mathsf{D}$ *are polytime with respect to* λ.
  3. $\mathsf{Gen}(1^{\lambda}) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$
  4. $\mathsf{E}(\mathsf{pk}, \mathsf{m}) \xrightarrow{\$} \mathsf{c}$ *with* $\mathsf{m} \in \{0,1\}^{\mathsf{n}}$, $\mathsf{c} \in \{0,1\}^{\mathsf{w}}$.
  5. $\mathsf{D}(\mathsf{sk}, \mathsf{c}) \to \mathsf{m}$ *or* $\perp$ *with* $\mathsf{m} \in \{0,1\}^{\mathsf{n}}$.
  6. *Given* $\mathsf{Gen}(1^{\lambda}) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$, $\forall \mathsf{x} \in \{0,1\}^{\mathsf{n}}$, $\mathsf{D}\big(\mathsf{sk}, \mathsf{E}(\mathsf{pk}, \mathsf{x})\big) = \mathsf{x}$
- $\mathsf{S}_{\mathsf{PKE}}$ *:*
  1. $\forall \mathsf{A}_1, \mathsf{A}_2$ $\mathsf{PPT}(\lambda)$

$$\mathsf{Adv}(\mathsf{A}_{1,2}^{\mathsf{C}}) := \left|\Pr\left[\mathsf{A}_2^{\mathsf{C}_{\mathsf{PKE}}}(\mathsf{c}, \mathsf{pk}, \mathsf{m}_0, \mathsf{m}_1, 1^{\mathsf{n}}, 1^{\mathsf{w}}) \to \mathsf{b} \;\middle|\; \begin{array}{c} \mathsf{Gen}(1^{\lambda}) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk}), \mathsf{b} \in_{\$} \{0,1\}, \\ \mathsf{A}_1^{\mathsf{C}_{\mathsf{PKE}}}(\mathsf{pk}, 1^{\mathsf{n}}, 1^{\mathsf{w}}) \xrightarrow{\$} (\mathsf{m}_0, \mathsf{m}_1), \mathsf{E}(\mathsf{pk}, \mathsf{m}_{\mathsf{b}}) \xrightarrow{\$} \mathsf{c} \end{array}\right] - \frac{1}{2}\right| \leqslant \mathsf{negl}(\lambda)$$

We have written these primitives because they will be very important later in this paper, but there exist many other usual examples, such as HomEnc (homomorphic encryption), FunEnc (functional encryption), commit (commitment scheme)...
Now that we have our primitives, let's define the notion of implementation, which can be seen as an interpretation of a primitive.

Definition 1.6 (Implementation)**.**
Given $\mathcal{P}$ a cryptographic primitive, an ***implementation*** C *is a list of number, sets, functions, relations and* PTM *such that :*

- C *is an interpretation of the variables* $\mathsf{C}_{\mathcal{P}}$
- *The formulas in* R *and* S *are satisfied when evaluated on* C*.*

We write C is an implementation of $\mathcal{P}$ *as* $\mathsf{C} \models \mathcal{P}$*.*
In the case where I *is not an implementation of* $\mathcal{P}$ *because it does not fulfill a condition in* S *due to an adversary* $\mathcal{A}$*, we write* $I \not\models_{\mathcal{A}} \mathcal{P}$ *and we say that* $\mathcal{A}$ ***breaks*** I*.*

Mathematicians will see that we are using the notation of a model satisfying a theory, which is rather appropriate, as we can indeed see $\mathsf{C}_{\mathcal{P}}$ as a language, $\mathsf{R}_{\mathcal{P}}$ and $\mathsf{S}_{\mathcal{P}}$ as a theory and C as a model. Therefore, cryptographic primitives can be seen through the lenses of higher order logic.

Note that if $\mathsf{C} \models \mathsf{PKE}$, then we have that it forms a semantically secure public key encryption scheme, usually called in literature an IND-CPA PKE scheme.

1.2 Reductions

Now that we have our primitives and their implementations, we have defined our object. As always in maths, object are nice, but we are missing relations between them. In our context, relations between primitives are call reductions.
There is a lot of different form of reductions. you can see a good varieties of those in [BBF13]. In this paper, we will only focus on just a tiny subset.

Definition 1.7 (Black-box reductions)**.**
Given $\mathcal{P}$, $\mathcal{Q}$, 2 crypto-primitives, we say that there exists a ***black-box reduction*** *from $\mathcal{P}$ to $\mathcal{Q}$, noted* $\left(\mathcal{P} \xhookrightarrow{BB} \mathcal{Q}\right)$ *if there exists* M, S*, two* PPT *such that for all* C*, for all* $\mathcal{A}$ *adversary:*

- ***correctness****:*
$$\mathsf{C} \models \mathcal{Q} \implies \mathsf{M}^{\mathsf{C}} \models \mathcal{P}$$
- ***security****:*
$$\mathsf{M}^{\mathsf{C}} \not\models_{\mathcal{A}^{\mathsf{M}^{\mathsf{C}}}} \mathcal{P} \implies \mathsf{C} \not\models_{\mathsf{S}^{\mathcal{A},\mathsf{C}}} \mathcal{Q}$$

Proposition 1.8 (Black-box composition)**.**
Let $\mathcal{P}, \mathcal{Q}, \mathcal{R}$ be primitives

$$\mathcal{P} \xhookrightarrow{BB} \mathcal{Q} \xhookrightarrow{BB} \mathcal{R} \implies \mathcal{P} \xhookrightarrow{BB} \mathcal{R}$$

Proof of Proposition 1.8:
Let M and S be the PPT used in $\mathcal{P} \xhookrightarrow{BB} \mathcal{Q}$ and N, T the one used in $\mathcal{Q} \xhookrightarrow{BB} \mathcal{R}$:

- **correctness**: We define O^{C} such that it simulates N^{C} and then simulate $\mathsf{M}^{\mathsf{N}^{\mathsf{C}}}$. We thus have that
$$\mathsf{C} \models \mathcal{R} \implies \mathsf{N}^{\mathsf{C}} \models \mathcal{Q} \implies \mathsf{M}^{\mathsf{N}^{\mathsf{C}}} = \mathsf{O}^{\mathsf{C}} \models \mathcal{P}$$
- **security**: We define $\mathsf{U}^{\mathcal{A},\mathsf{C}}$ such that it first runs $S^{\mathcal{A},\mathsf{N}^{\mathsf{C}}}$, then $T^{S^{\mathcal{A}},C}$ and thus
$$\mathsf{O}^{\mathsf{C}} = \mathsf{M}^{\mathsf{N}^{\mathsf{C}}} \not\models_{\mathcal{A}^{\mathsf{O}^{\mathsf{C}}}} \mathcal{P} \implies \mathsf{N}^{\mathsf{C}} \not\models_{\mathsf{S}^{\mathcal{A},\mathsf{N}^{\mathsf{C}}}} \mathcal{Q} \implies \mathsf{N}^{\mathsf{C}} \not\models_{\mathsf{T}^{\mathsf{S}^{\mathcal{A}},\mathsf{C}}} \mathcal{R}$$

□ 1.8

Let's see a few examples:

Example 1.9 ($\mathsf{polyTDF}$ and $\mathsf{polyTDF}$)**.**
We define the primitive $\mathsf{polyTDF}$ *as the triplet form* $(\mathsf{C}_{\mathsf{TDF}}, \mathsf{R}', \mathsf{S}_{\mathsf{TDF}})$*, with* R' *defined* R *with the added following requirement:*

$$\forall \mathsf{u} \in \{0,1\}^*, \ \left|\left\{(\mathsf{k},\mathsf{x})\middle|\mathsf{F}(\mathsf{k},\mathsf{x}) = \mathsf{u}\right\}\right| = \mathsf{poly}(\lambda)$$

We see that trivially, $\mathsf{TDF} \xhookrightarrow{\mathsf{BB}} \mathsf{polyTDF}$ *using* $\mathsf{M}^{\mathsf{C}} = \mathsf{C}$ *and* $\mathsf{S}^{\mathcal{A},\mathsf{C}} = \mathcal{A}^{\mathsf{C}}$

Example 1.10 (wPKE)**.**
We define the primitive wTDF*, of weak* PKE *as follows:*

- $\mathsf{C}_{\mathsf{wPKE}} = \left[\mathsf{n}, \mathsf{w}, \mathsf{Gen}, \mathsf{E}, \mathsf{D}\right]$
- $\mathsf{R}_{\mathsf{wPKE}}$ *is composed of the following requirements:*
  1. $\mathsf{w}, \mathsf{Gen}, \mathsf{E}, \mathsf{D}$ *are* $\mathsf{poly}(\mathsf{n})$.
  2. $\mathsf{Gen}(1^{\mathsf{n}}) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$

3. $\mathsf{E}(\mathsf{pk},\mathsf{m}) \xrightarrow{\$} \mathsf{c}$ *with* $\mathsf{m} \in \{0,1\}^{\mathsf{n}}$, $\mathsf{c} \in \{0,1\}^{\mathsf{w}}$.
4. $\mathsf{D}(\mathsf{sk},\mathsf{c}) \rightarrow \mathsf{m}$ *or* $\perp$.
5. *Given* $\mathsf{Gen}(1^{\mathsf{n}}) \xrightarrow{\$} (\mathsf{sk},\mathsf{pk})$, $\forall \mathsf{x} \in \{0,1\}^{\mathsf{n}}$, $\mathsf{D}\big(\mathsf{sk},\mathsf{E}(\mathsf{pk},\mathsf{x})\big) = \mathsf{x}$

- $\mathsf{S}_{\mathsf{wPKE}}$ *:*
  1. $\forall \mathsf{A}$ $\mathsf{PPT}(\mathsf{n})$

$$\Pr\left[\mathsf{A}^{\mathsf{C}_{\mathsf{wPKE}}}(\mathsf{c},\mathsf{pk},1^{\mathsf{n}}) \rightarrow \mathsf{m} \;\middle|\; \mathsf{Gen}(1^{\mathsf{n}}) \xrightarrow{\$} (\mathsf{sk},\mathsf{pk}), \mathsf{m} \in_{\$} \{0,1\}^{\mathsf{n}}, \mathsf{E}(\mathsf{pk},\mathsf{m}) \xrightarrow{\$} \mathsf{c}\right] \leqslant \mathsf{negl}(\mathsf{n})$$

wPKE are usually seen inside literature as OW-CPA PKE.

Lemma 1.11.

$$\mathsf{wPKE} \overset{\mathsf{BB}}{\hookrightarrow} \mathsf{PKE}$$

Proof of Lemma 1.14:
We have to define the M and S for our blackbox reduction.

M^{C}**:**
$n_{\mathsf{wPKE}} \leftarrow n_{\mathsf{PKE}}$
$w_{\mathsf{wPKE}} \leftarrow w_{\mathsf{PKE}}$
$\mathsf{KG}_{\mathsf{wPKE}}(1^{\mathsf{n}}) \leftarrow_{\$} \mathsf{KG}_{\mathsf{PKE}}(1^{\lambda})$
$\mathsf{E}_{\mathsf{wPKE}}(\mathsf{pk},\mathsf{n}) \leftarrow_{\$} \mathsf{E}_{\mathsf{PKE}}(\mathsf{pk},\mathsf{n})$
$\mathsf{D}_{\mathsf{wPKE}}(\mathsf{sk},\mathsf{c}) \leftarrow_{\$} \mathsf{D}_{\mathsf{PKE}}(\mathsf{sk},\mathsf{c})$

$\mathcal{S}_1^{\mathcal{A},\mathsf{C}}(\mathsf{pk},1^{\mathsf{n}},1^{\mathsf{w}})$**:**
$\mathsf{m}_0,\mathsf{m}_1 \in_{\$} \{0,1\}^{\mathsf{n}}$
return $(\mathsf{m}_0,\mathsf{m}_1)$

$\mathcal{S}_2^{\mathcal{A},\mathsf{C}}(\mathsf{c},\mathsf{pk},\mathsf{m}_0,\mathsf{m}_1,1^{\mathsf{n}},1^{\mathsf{w}})$**:**
$x' \leftarrow \mathcal{A}^{\mathsf{C}}(\mathsf{pk},\mathsf{c},1^{\mathsf{n}})$
if $x' = m_0$ **then**
  return 0
end
else if $x' = m_1$ **then**
  return 1
end
return $b' \in_{\$} \{0,1\}$

We first see that we $\mathcal{S}_1^{\mathcal{A},\mathsf{C}}(\mathsf{pk},1^{\mathsf{n}},1^{\mathsf{w}})$ and $\mathcal{S}_2^{\mathcal{A},\mathsf{C}}(\mathsf{c},\mathsf{pk},\mathsf{m}_0,\mathsf{m}_1,1^{\mathsf{n}},1^{\mathsf{w}})$ are symmetric with respect to b and thus, for the sake of presentation, we will assume that $b = 1$.

$$\begin{aligned}
\mathsf{Adv}(\mathrm{S}_{1,2}^{\mathcal{A},\mathsf{C}}) &= \Pr\left[\mathcal{S}_2^{\mathcal{A},\mathsf{C}}(\tilde{c}, \mathsf{pk}, \mathsf{m}_0, \mathsf{m}_1, 1^{\mathsf{n}}, 1^{\mathsf{w}}) = 1 | \mathsf{b} = 1\right] - \frac{1}{2} \\
&= \Pr\left[\mathcal{S}_2^{\mathcal{A},\mathsf{C}}(\tilde{c}, \mathsf{pk}, \mathsf{m}_0, \mathsf{m}_1, 1^{\mathsf{n}}, 1^{\mathsf{w}}) = 1 | \mathsf{b} = 1, \mathsf{A}^{\mathsf{C}}(\mathsf{pk}, \mathsf{c}, 1^{\mathsf{n}}) \text{ works}\right] \Pr\left[\mathsf{A}^{\mathsf{C}}(\mathsf{pk}, \mathsf{c}, 1^{\mathsf{n}}) \text{ works}\right] - \frac{1}{2} \\
&+ \Pr\left[\mathcal{S}_2^{\mathcal{A},\mathsf{C}}(\tilde{c}, \mathsf{pk}, \mathsf{m}_0, \mathsf{m}_1, ...) = 1 | \mathsf{b} = 1, \mathsf{A}^{\mathsf{C}}(\mathsf{pk}, \mathsf{c}, 1^{\mathsf{n}}) \text{does not works}\right] \Pr\left[\mathsf{A}^{\mathsf{C}}(\mathsf{pk}, \mathsf{c}, 1^{\mathsf{n}}) \text{does not works}\right] \\
&= \mathsf{Adv}(\mathsf{A}^{\mathsf{C}}) + \frac{1}{2}\left(1 - \mathsf{Adv}(\mathsf{A}^{\mathsf{C}})\right) - \frac{1}{2} \\
&= \frac{1}{2}\mathsf{Adv}(\mathsf{A}^{\mathsf{C}}) \\
&> \mathsf{negl}(\mathsf{n})
\end{aligned}$$

□ 1.14

Another important blackbox reduction is the following one.

Theorem 1.12.

$$\mathsf{PKE} \xhookrightarrow{\mathsf{BB}} \mathsf{polyTDF}$$

Proof of Theorem 1.12:
Can be found here [Yao82] and [BHSV98].

□ 1.12

Other types of blackbox reductions exists. We will use a slightly weaker one than 1.7, defined as follows:

Definition 1.13 (Strong semi black-box reductions)**.**
Given $\mathcal{P}$, $\mathcal{Q}$, 2 crypto-primitives, we say that there exists a ***strong semi black-box reduction*** *from $\mathcal{P}$ to $\mathcal{Q}$, noted $\left(\mathcal{P} \xhookrightarrow{BNB} \mathcal{Q}\right)$ if there exists M, for all adversary $\mathcal{A}$, exists $\mathsf{S}_{\mathcal{A}}$ such that for all C :*

- ***correctness:***
$$\mathsf{C} \models \mathcal{Q} \implies \mathsf{M}^{\mathsf{C}} \models \mathcal{P}$$
- ***security:***
$$\mathsf{M}^{\mathsf{C}} \not\models_{\mathcal{A}^{\mathsf{M}^{\mathsf{C}}}} \mathcal{P} \implies \mathsf{C} \not\models_{\mathsf{S}_{\mathcal{A}}^{\mathcal{A},\mathsf{C}}} \mathcal{Q}$$

Here, the notation BNB is taken from [BBF13].

Lemma 1.14.

$$\mathsf{PKE} \xhookrightarrow{\mathsf{BNB}} \mathsf{wPKE}$$

Proof of Lemma 1.14:
We set the following values:

$$\begin{aligned}\lambda_{\mathsf{PKE}} &\leftarrow \mathsf{n}_{\mathsf{wPKE}}\\ \mathsf{n}_{\mathsf{PKE}} &\leftarrow 1\\ \mathsf{w}_{\mathsf{PKE}} &\leftarrow 1 + \mathsf{n}_{\mathsf{wPKE}} + \mathsf{w}_{\mathsf{wPKE}}\end{aligned}$$

KG, E and D are then defined as such:

$\mathsf{KG}^{\mathsf{C}}_{\mathsf{PKE}}(1^\lambda)$**:**	$\mathsf{E}^{\mathsf{C}}_{\mathsf{PKE}}(\mathsf{pk}, \mathsf{b})$**:**	$\mathsf{D}^{\mathsf{C}}_{\mathsf{PKE}}(\mathsf{sk}, \mathsf{c})$**:**
$(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{KG}_{\mathsf{wPKE}}(1^{\mathsf{n}})$	$\mathsf{x} \leftarrow_\$ \{0,1\}^{\mathsf{n}_{\mathsf{wPKE}}}$	$\mathsf{c}_1 \\| \mathsf{c}_2 \\| \mathsf{r} \leftarrow \mathsf{c}$
return $(\mathsf{sk},\mathsf{pk})$	$\mathsf{r} \leftarrow_\$ \{0,1\}^{\mathsf{n}_{\mathsf{wPKE}}}$	$\mathsf{x} \leftarrow \mathsf{D}_{\mathsf{wPKE}}(\mathsf{sk}, \mathsf{c}_2)$
	$\mathsf{c}_1 \leftarrow_\$ \mathsf{b} \oplus (\mathsf{x} \bigodot \mathsf{r})$	**return** $\mathsf{c}_1 \oplus (\mathsf{x} \bigodot \mathsf{r})$
	return $\mathsf{c}_1 \\| \mathsf{E}_{\mathsf{wPKE}}(\mathsf{pk}, \mathsf{x}) \\| \mathsf{r}$	

We thus have to show that an if C is an implementation of wPKE, then M^{C} is an implementation of wPKE. This comes from the fact that this is the Goldreich-Levin construction ([GL89], [HJKS10]) which garanties indistinguisability provided it is given a one-way function and because C is an implementation of wPKE, we have that $\mathsf{E}_{\mathsf{wPKE}}$ is one.[2]
The proof of the security part follows from what is defined in [GL89], [HJKS10] and [BBF13].

□ 1.14

Blackbox reduction is a huge family of reduction, but it is not the only one. Some are strictly based on oracles. They are an interesting notion because oracles have many advantages, as they are usually easier to work with and we do not have any requirement about computation time.

Definition 1.15 (Relativisation reductions)**.**
Given $\mathcal{P}$, $\mathcal{Q}$, 2 crypto-primitives, we say that there exists a ***relativizing reduction*** *from $\mathcal{P}$ to $\mathcal{Q}$, noted $\left(\mathcal{P} \xhookrightarrow{*} \mathcal{Q}\right)$ if there exists M such that for all C, for all Π:*

$$\mathsf{C}^{\Pi} \models \mathcal{Q}^{\Pi} \implies \mathsf{M}(\mathsf{C})^{\Pi} \models \mathcal{P}^{\Pi}$$

[2] We can see $\mathsf{E}_{\mathsf{wPKE}}$ as a function if it is given its randomness.

where $\mathcal{P}^{\Pi}$ *is* $\mathcal{P}$*, where all* TM*s (meaning both variables and adversaries) have oracle access to* Π.
By $\mathsf{M}(\mathsf{C})$*, we denote the fact that* M *is given the "code" of* C *and not just a blackbox.*

If the correctness part is quite apparent, it may seems that we have dropped the security part, but we have not. It is "hidden". If we have an adversary $\mathcal{A}$ that break $M(C)$, then by choosing $\mathcal{A}$ as our oracle, we have that $M(C)^{\mathcal{A}} \not\models_{\mathcal{A}} \mathcal{P}^{\mathcal{A}}$, inducing that we are required that there exist an adversary $\mathcal{S}$ such that $C \not\models_{\mathcal{S}^{\mathcal{A}}} \mathcal{G}^{\mathcal{A}}$.
There exists a huge family of relativisation reductions. See [RTV04] for further study.

Proposition 1.16.
Let $\mathcal{P}, \mathcal{Q}$ *be primitives. Then*

$$\mathcal{P} \xhookrightarrow{BB} \mathcal{Q} \implies \mathcal{P} \xhookrightarrow{BNB} \mathcal{Q}$$

$$\mathcal{P} \xhookrightarrow{BNB} \mathcal{Q} \implies \mathcal{P} \xhookrightarrow{*} \mathcal{Q}$$

Proof of Proposition 1.16:

- This simply comes from the fact that we can set for every adversary $\mathsf{S}_{\mathcal{A}}$ to be simply S.
- We assume that we have a strong semi black-box reduction but no relativisation reduction between $\mathcal{P}$ to $\mathcal{Q}$. This means that

  $$\forall M, \exists C, \exists \Pi\ \exists \mathsf{A} \text{ s.t. } \mathsf{C}^{\Pi} \models \mathcal{Q}^{\Pi} \wedge \mathsf{M}(\mathsf{C})^{\Pi} \not\models_{\mathcal{A}^{\mathsf{C}^{\Pi}},\Pi} \mathcal{P}^{\Pi}$$

  First, we see that $\mathcal{A}^{\mathsf{C}^{\Pi},\Pi} = \mathcal{A}^{\mathsf{C},\Pi}$. Secondly, we take $\mathsf{M}, \mathsf{S}_{\mathsf{A}}$ given by the strong semi black-box reduction of $\mathcal{P}$ to $\mathcal{Q}$, with C and Π such that the previous formula holds, by seeing $M(C)^{\Pi}$ as $M^{C^{\Pi}}$.

  Then, consider the adversary that runs $\mathcal{B}^{C^{\Pi},\Pi} = \mathsf{S}_{\mathcal{A}}^{\mathcal{A}^{\Pi},\mathsf{C}}$ and we have, by the property of S_{A} that $C^{\Pi} \not\models_{\mathsf{S}^{\mathcal{A}^{\Pi},\mathsf{C}}} \mathcal{Q}^{\Pi}$, which contradicts our initial assertion.

□ 1.16

Note that the converse of both implication are not true. A proof is given in [BBF13].

1.3 Separations

Now that we have our notions of reductions, we want to define a method to show **separation**, meaning the impossibility of reductions between primitives. We are mainly interested into separations of black-box reductions. At first, we could just consider the negation of black-box reductions, but it is rather cumbersome to work with.

By 1.16, we have that $\mathcal{P} \overset{*}{\not\to} \mathcal{Q} \implies \mathcal{P} \overset{BB}{\not\to} \mathcal{Q}$. This gives us our first non trivial separation method, which is historically the first one to provide interesting results. [IR89],[Sim98], [RTV04].

Definition 1.17 (Relative Separation)**.**
Given $\mathcal{P}$, $\mathcal{Q}$, two crypto-primitives, we have that their is no black-box reductions between $\mathcal{P}$ and $\mathcal{Q}$ if

$$\forall M\ \exists C\ \exists \Pi\ s.t.\ C^{\Pi} \models \mathcal{Q}^{\Pi} \wedge M(C)^{\Pi} \not\models \mathcal{P}^{\Pi}$$

This is a first step, but the problem is that we are working on relativisation separations, which are more difficult than blackbox separation.
Hence, in [HR04], Hsiao and Reyzin introduced a way to see black-box separation using tools of relativisation separation. This method is called the **two-oracles separation**:

Definition 1.18 (Classic two-oracles separation)**.**
Given $\mathcal{P}$, $\mathcal{Q}$, two crypto-primitives, we have that their are no black-box reductions between $\mathcal{P}$ and $\mathcal{Q}$, $\mathcal{P} \overset{BB}{\not\to} \mathcal{Q}$ if there exists two oracles Ω and Π such that there exists C, for all M :

1. $\mathsf{C}^{\Omega} \models \mathcal{Q}^{\Omega}$
2. $\mathsf{M}^{\Omega} \not\models_{\Pi} \mathcal{P}^{\Omega,\Pi}$
3. $\mathsf{C}^{\Omega} \models \mathcal{Q}^{\Omega,\Pi}$

with Π_M being a small abuse of notation, as it represent $\not\models_{\mathcal{A}^{\Pi}}$, with $\mathcal{A}$ an adversary that only query Π. Usually, C is made to be very simple with most of the work done by the oracle Ω.

We thus give a valid implementation of $\mathcal{Q}$ using Ω and a way to break any black-box transform of this implementation using Π such that this breaker is still not strong enough to break $\mathcal{Q}$. The usage of oracles allows to not have to consider computational time. This separation technique was used in [DOP05], [FS12], [FLR$^+$10].

Using 1.18 as an inspiration, [GMR01] derived another two way separation which is the backbone of their paper.

Definition 1.19 (Two-oracles separation)**.**
Given $\mathcal{P}$, $\mathcal{Q}$, two crypto-primitives, we have that their are no strong semi black-box reductions between $\mathcal{P}$ and $\mathcal{Q}$, $\mathcal{P} \overset{BNB}{\not\hookrightarrow} \mathcal{Q}$ if there exists an of oracle Ω the ***implementer****, there exists C such that:*

1. $\mathsf{C}^{\Omega} \models \mathcal{Q}^{\Omega}$
2. $\forall \mathsf{M},\ \mathsf{M}^{\Omega} \models \mathcal{P}^{\Omega} \implies \exists \Pi_{\mathsf{M}}, \mathsf{M}^{\Omega} \not\models_{\Pi_{\mathsf{M}}} \mathcal{P}^{\Omega,\Pi_{\mathsf{M}}}$
3. $\mathsf{C}^{\Omega} \models \mathcal{Q}^{\Omega,\Pi_{\mathsf{M}}}$

Π_{M} *are called the* ***breakers****.*

The main difference between 1.18 and 1.19 is that here Π can adapt to M.

Verification of Definition 1.19:
Let's assume that we have $\mathcal{P} \xhookrightarrow{BNB} \mathcal{Q}$ using $\mathsf{M}, \mathsf{S}_{\mathsf{A}}$. Then, we can see $\mathsf{M}^{\mathsf{C}^{\Omega}}$ as M^{Ω} and thus $\mathsf{M}^{\mathsf{C}^{\Omega}} \models \mathcal{P}^{\Omega}$, meaning that $\mathsf{M}^{\mathsf{C}^{\Omega}} \not\models_{\Pi_{\mathsf{M}}} \mathcal{P}^{\Omega,\Pi_{\mathsf{M}}}$. Then, seeing $\mathsf{S}_{\Pi_{\mathsf{M}}}^{\mathcal{A}^{\Pi_{\mathsf{M}}},\mathsf{C}^{\Omega}}$ as $S_{\Pi_M}^{\Pi_M,\Omega}$, we would have that $\mathsf{C}^{\Omega} \not\models_{\mathsf{S}_{\Pi_{\mathsf{M}}}^{\mathcal{A}^{\Pi_{\mathsf{M}}},\mathsf{C}^{\Omega}}} \mathcal{Q}^{\Omega,\Pi_{\mathsf{M}}}$, breaking the fact that $\mathsf{C}^{\Omega} \models \mathcal{Q}^{\Omega,\Pi_{\mathsf{M}}}$.

$\square$ 1.19

Now that we have dust off our field and seen the necessary requirement, we can trough ourself into our proof.

2 Objects definitions

Let's now state our main theorem, initialy stated in [GMR01].

Theorem 2.1 (Separation of $\mathsf{polyTDF}$ and PKE)**.**

$$\mathsf{polyTDF} \overset{\mathsf{BB}}{\not\to} \mathsf{PKE}$$

To show such a result, we will start with a small observation

Proposition 2.2.

$$\mathsf{polyTDF} \overset{\mathsf{BNB}}{\not\to} \mathsf{wPKE} \implies \mathsf{polyTDF} \overset{\mathsf{BB}}{\not\to} \mathsf{PKE}$$

Proof of Proposition 2.2:
Assume that $\mathsf{polyTDF} \overset{\mathsf{BNB}}{\not\to} \mathsf{wPKE}$ and that $\mathsf{polyTDF} \xhookrightarrow{\mathsf{BB}} \mathsf{PKE}$. We are thus, using 1.16 in the following diagram

$$\begin{tikzcd}
\mathsf{wPKE} & \\
\mathsf{PKE} \arrow[u, "\mathsf{BNB}"] & \mathsf{polyTDF} \arrow[l, "\mathsf{BNB}"'] \arrow[ul, bend right, "/" description]
\end{tikzcd}$$

Which contradicts the associativity of BNB, which is proved exactly like in 1.8.

□ 2.2

Therefore, it suffice to separate $\mathsf{polyTDF}$ from wPKE to separate them from PKE. Thus, we will focus on the following theorem.

Theorem 2.3.

$$\mathsf{polyTDF} \overset{\mathsf{BNB}}{\not\to} \mathsf{wPKE}$$

Proof of Theorem 2.3:
This is given by using the two-oracle separation 1.19 and the merging 2.7, 3.6 and 4.10.

□ 2.3

To use 1.19, we requires two oracles that we defined as 2.5 and 2.12. The following subsections are dedicated to their definitions.

2.1 The oracle Ω

Definition 2.4 (the Ω oracle)**.**
Ω is composed of a triplet of oracle $\langle \mathsf{G}, \mathsf{E}, \mathsf{D} \rangle$ such that on any n

- $\mathsf{G} : \{0,1\}^{\mathsf{n}} \to \{0,1\}^{3\mathsf{n}}$ *a random length tripling function with* $\mathsf{G}(\mathsf{sk}) = \mathsf{pk}$.
- $\mathsf{E} : \{0,1\}^{5\mathsf{n}} \to \{0,1\}^{4\mathsf{n}}$ *a random function with* $\mathsf{E}(\mathsf{pk}, \mathsf{r}, \mathsf{m}) = \mathsf{c}$ *such that for all* pk, $\mathsf{E}(\mathsf{pk}, *, *)$ *is injective with* $\mathsf{m}, \mathsf{r} \in \{0,1\}^{\mathsf{n}}$
- D *a deterministic decryption such that for* $\mathsf{G}(\mathsf{sk}) = \mathsf{pk}$, $\mathsf{E}(\mathsf{pk}, \mathsf{r}, \mathsf{m}) = \mathsf{c}$ *we have that* $\mathsf{D}(\mathsf{sk}, \mathsf{c}) \to \mathsf{m}$. *otherwise, it outputs* $\perp$

Definition 2.5 (Our C^{Ω} implementation)**.**
We define our C^{Ω} in the following way:

- $\mathsf{w} = 4\mathsf{n}$.
- $\mathsf{Gen}^{\Omega}(1^{\mathsf{n}})$ *that sample* $\mathsf{sk} \in_{\$} \{0,1\}^{\mathsf{n}}$ *and return* $\big(\mathsf{sk}, \mathsf{G}_{\Omega}(\mathsf{sk})\big)$.
- $\mathsf{E}^{\Omega}(\mathsf{pk}, \mathsf{m})$ *that sample* $\mathsf{r} \in_{\$} \{0,1\}^{\mathsf{n}}$ *and return* $\mathsf{E}_{\Omega}(\mathsf{pk}, \mathsf{r}, \mathsf{m})$.
- $\mathsf{D}^{\Omega}(\mathsf{sk}, \mathsf{c})$ *that simply return* $\mathsf{D}_{\Omega}(\mathsf{sk}, \mathsf{c})$.

Remark 2.6.

- For any $\mathsf{c} \in_{\$} \{0,1\}^{4\mathsf{n}}$, $\Pr[\mathsf{c} \in \mathsf{E}_{\Omega}(\mathsf{pk}, *, *)] = \frac{1}{4^{\mathsf{n}}}$
- Given any c, for any $\mathsf{sk} \in_{\$} \{0,1\}^{\mathsf{n}}$, $\Pr[\mathsf{D}^{\Omega}(\mathsf{sk}, \mathsf{c}) \neq \perp] = \Pr[\mathsf{D}_{\Omega}(\mathsf{sk}, \mathsf{c}) \neq \perp] = \frac{1}{4^{\mathsf{n}}}$
- For $\mathsf{pk} \in_{\$} \{0,1\}^{3\mathsf{n}}$, $\Pr[\mathsf{G}_{\Omega}(*) = \mathsf{pk}] = \frac{1}{4^{\mathsf{n}}}$

Lemma 2.7.

$$\mathsf{C}^{\Omega} \models \mathsf{wPKE}^{\Omega}$$

Proof of Lemma 2.7:
Let's show that C^{Ω} follows $\mathsf{R}_{\mathsf{wPKE}^{\Omega}}$ and $\mathsf{S}_{\mathsf{wPKE}^{\Omega}}$, defined in 1.10.

- Showing point 1 to 4 of $\mathsf{R}_{\mathsf{wPKE}^{\Omega}}$ is trivial. The fact that point 5 hold is because we asked for $\mathsf{E}_{\Omega}(\mathsf{pk}, *, *)$ to be injective. This means that given pk, c is the image of only at most one message m, making D_{Ω} possible, and thus D^{Ω} is a perfect decryption.

- Now, what remains to show is that for all A a $\mathsf{PPT(n)}$

  $$\Pr\left[\mathsf{A}^{\mathsf{C}_{\mathsf{wPKE}},\Omega}(\mathsf{c}, \mathsf{pk}, 1^{\mathsf{n}}) \to \mathsf{m} \;\middle|\; \mathsf{Gen}^{\Omega}(1^{\mathsf{n}}) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk}), \mathsf{E}^{\Omega}(\mathsf{pk}, \mathsf{m}) \xrightarrow{\$} \mathsf{c}, \mathsf{m} \in_{\$} \{0,1\}^{\mathsf{n}}\right] \leqslant \mathsf{negl(n)}$$

  We will show that we have perfect secrecy. More precisely, we have that c, pk is independant from m, sk ($\mathsf{c}, \mathsf{pk} \perp\!\!\!\perp \mathsf{m}, \mathsf{sk}$). Indeed:

  - As $\mathsf{m} \perp\!\!\!\perp \mathsf{sk}$ and $\mathsf{pk} = \mathsf{G}_{\Omega}(\mathsf{sk})$, we have that $\mathsf{m} \perp\!\!\!\perp \mathsf{pk}$.
  - As G_{Ω} is a random function, we have $\mathsf{sk} \perp\!\!\!\perp \mathsf{pk}$.
  - Similarly, because E_{Ω} is a random, we have that $\mathsf{c} \perp\!\!\!\perp \mathsf{pk}, \mathsf{m}$.
  - $\mathsf{m}, \mathsf{pk}, \mathsf{r} \perp\!\!\!\perp \mathsf{sk}$ implies that $\mathsf{c} \perp\!\!\!\perp \mathsf{sk}$

  Thus $\Pr\left[\mathsf{m} = \mathsf{x}, \mathsf{sk} = \mathsf{y} \middle| \mathsf{c} = \mathsf{a}, \mathsf{pk} = \mathsf{b}\right] = \Pr\left[\mathsf{m} = \mathsf{x}, \mathsf{sk} = \mathsf{y}\right]$ making C^{Ω} perfectly secure.

  Furthermore, querying other values only improve negligibly our knowledge of sk and m. Indeed,

  - Because G_{Ω} is random, then for $\mathsf{G}_{\Omega}(\mathsf{sk}') = \mathsf{pk}'$, if $\mathsf{pk}' \neq \mathsf{pk}$, then we only gain information that $\mathsf{sk}' \neq \mathsf{sk}$, meaning that $2^n - 1$ possibilities remain.
  - Because E_{Ω} is a random injective function, then for $\mathsf{E}_{\Omega}(\mathsf{pk}, \mathsf{r}', \mathsf{m}') = \mathsf{c}'$, if $\mathsf{c}' \neq \mathsf{c}$, then we only gain information that $(\mathsf{r}', \mathsf{m}') \neq (\mathsf{r}, \mathsf{m})$, meaning that $4^n - 1$ possibilities remain to be checked.
  - Because D_{Ω} follows from G_{Ω} and E_{Ω}, with probability $1 - \frac{1}{4^n}$ we have that $\mathsf{D}_{\Omega}(\mathsf{sk}', \mathsf{c}) = \perp$, then we only gain information that $\mathsf{sk}' \neq \mathsf{sk}$, meaning that $2^n - 1$ possibilities remain to be checked.

  Therefore, we have that for all $\mathcal{A}^{\Omega}$ computationally unbounded but $\mathsf{poly(n)}$ querying adversary,

  $$\begin{aligned}\mathsf{Adv}(\mathcal{A}^{\Omega}) &\leqslant \Pr\left[\mathcal{A}^{\Omega} \text{ queries } \mathsf{G}(\mathsf{sk}), \mathsf{E}(\mathsf{pk}, \mathsf{r}, \mathsf{m}) \text{ or } \mathsf{D}(\mathsf{sk}, \mathsf{c})\right] \\ &\leqslant \frac{\mathsf{poly(n)}}{2^n} \\ &\leqslant \mathsf{negl(n)}\end{aligned}$$

□ 2.7

We can rejoice in the fact that we have showed the first part of our theorem 2.3. The following part requires us to define Π_M.

2.2 The oracles Π_M

We now want to define our Π_M. To do so, we will work on M^Ω an implementation of $\mathsf{polyTDF}$. Before being able to define Π_M, we need to give a bit of structure to M^Ω, namely

Lemma 2.8.
Consider $\mathsf{M}^\Omega = \langle \lambda, \mathsf{n}, \mathsf{KG}^\Omega, \mathsf{F}^\Omega, \mathsf{T}^\Omega \rangle$. *wlog, we can assume that:*

1. $\lambda = \mathsf{n}$
2. KG^Ω *does not query* D_Ω
3. *When* F^Ω *queries* $\mathsf{D}_\Omega(\mathsf{sk}, \mathsf{c})$*, it first queries* $\mathsf{G}_\Omega(\mathsf{sk})$.
4. $\mathsf{KG}^\Omega(1^\mathsf{n}) = (\mathsf{k}, \mathsf{tk})$ *with* $\mathsf{k} \in \{0,1\}^\mathsf{n}$ *and* tk *is the query-list of* $\mathsf{KG}^\Omega(1^\mathsf{n})$.[3]
5. $\mathsf{T}^\Omega(\mathsf{tk}, \mathsf{y})$ *does not make queries if the desired information is already in* tk.
6. *there exists* $\alpha > 0$ *such that* $\mathsf{KG}^\Omega, \mathsf{F}^\Omega, \mathsf{T}^\Omega$ *all run in time at most* n^α.
7. F^Ω *is* n^α*-to-one.*

Proof of Lemma 2.8:

1. By our definition, $\mathsf{n} = \mathsf{poly}(\lambda)$ with λ which doesn't change our security analysis. This is thus done for the sake of clarity.
2. If KG^Ω queries $\mathsf{D}_\Omega(\mathsf{sk}, \mathsf{c})$. Then either:
   - it knows that c is a ciphertext and because it was given by G_Ω and E_Ω, making a queries and answer to D_Ω is superfluous.
   - it does not know if c is a ciphertext, but as seen in 2.6, calling D_Ω will give insightful information with negligible probability. We can thus drop it.
3. This hold for the same reason as the last point. Calling $\mathsf{D}_\Omega(\mathsf{sk}, \mathsf{c})$ without querying $\mathsf{G}_\Omega(\mathsf{sk})$ first induce that we do not know if c is a ciphertext or not.
4. Due to the security parameter being n, we can restrict ourself to have 2^n possible coubles $(\mathsf{k}, \mathsf{tk})$. We can thus consider that they all lie in $\{0,1\}^n$. For the fact that tk is the query list of KG^Ω, this comes from the fact that k and tk is computed using those queries in polytime. We can thus move this construction to T^Ω.
5. If $\mathsf{T}^\Omega(\mathsf{tk}, \mathsf{y})$ needs a query in tk, then it could just have looked in tk.

[3] With the notion of query-list defines in 2.9

6. As they are polysize over finite sets. Using the cofinality of $\mathbb{N}$, we have that such an α exists.

7. As they are poly-to-one over finite sets. Using the cofinality of $\mathbb{N}$, we have that such an α exists.

□ 2.8

Before defining our oracle, we need a view definitions on how to handle queries.

Definition 2.9 (Query list and oracle consistency).

- *Given* $\mathbf{O} = \langle \mathsf{O}_1, \cdots, \mathsf{O}_\mathsf{n} \rangle$, *the* ***query list*** *of* $\mathsf{M}^{\mathbf{O}}$ *on* x, *noted* $\mathsf{QL}(\mathsf{M}^{\mathbf{O}}(\mathsf{x})) = \big[(\mathsf{q}, \mathsf{i}, \mathsf{x})_\mathsf{l}\big]_{\mathsf{l} \in [\mathsf{QL}]}$ *of all queries made by* M *to* $\mathbf{O}$ *such that* $\mathsf{x}_\mathsf{l} = \mathsf{O}_{\mathsf{i}_\mathsf{l}}(\mathsf{q}_\mathsf{l})$.
- *A list* L *is an* ***O-list*** *if it is in the form* $\mathsf{L} = [(\mathsf{q}, \mathsf{i}, \mathsf{x})_\mathsf{l}]_{\mathsf{l} \in [\mathsf{L}]}$ *with* $\mathsf{x}_\mathsf{l} = \mathsf{O}_{\mathsf{i}_\mathsf{l}}(\mathsf{q}_\mathsf{l})$.
- *An oracle list* $\mathbf{O}$ *is* ***consistent*** *with* L *of the form* $\mathsf{L} = [(\mathsf{q}, \mathsf{i}, \mathsf{x})_\mathsf{l}]_{\mathsf{l} \in [\mathsf{L}]}$ *if* $\mathsf{x}_\mathsf{l} = \mathsf{O}_{\mathsf{i}_\mathsf{l}}(\mathsf{q}_\mathsf{l})$.

We now define two very specific notions

Definition 2.10 (Informative sublists).

- *Let* L_1 *be a* E_Ω*-list and let* L_2 *be a* D_Ω*-list. We say that* $\mathsf{L}_2 \prec \mathsf{L}_1$ *if*

$$\big((\mathsf{sk}, \mathsf{c}), \mathsf{m}\big) \in \mathsf{L}_2 \implies \exists \mathsf{r}, \big((\mathsf{G}_\Omega(\mathsf{sk}), \mathsf{r}, \mathsf{m}), \mathsf{c}\big) \in \mathsf{L}_1$$

- *Given* $\widehat{\Omega}$ *a oracle similar to* Ω *and a list* $\mathbf{L}$. *We say that a query* $(\mathsf{sk}, \mathsf{c})$ *to* $\mathsf{D}_{\widehat{\Omega}}$ *made by* $\mathsf{T}^{\widehat{\Omega}}(\mathsf{tk}', \mathsf{y})$ *is* ***informative with respect to L*** *if:*
  1. $\mathsf{D}_{\widehat{\Omega}}(\mathsf{sk}, \mathsf{c}) \neq \perp$
  2. $\mathsf{T}^{\widehat{\Omega}}$ *did not previously query* $\mathsf{E}_{\widehat{\Omega}}(\mathsf{G}_{\widehat{\Omega}}(\mathsf{sk}), *, *) = \mathsf{c}$
  3. $(*, 2, \mathsf{c}) \notin \mathsf{L}$

We can now use those definition to define another oracle $\widetilde{\Omega}$, the cornerstone of Π.

Definition 2.11 (The oracle $\widetilde{\Omega}_k$).
For a given k, *we define:*

1. *Let* $\mathsf{l_1}, \mathsf{l_2}$ *be* $\mathsf{poly(n)}$*. Let* $\mathsf{u_1}, \cdots, \mathsf{u_{l_1}}$ *be random* n*-bit strings.*

$$\mathsf{L_k} = \bigcup_{\mathsf{j} \in [\mathsf{l_1}]} \mathsf{QL}\big(\mathsf{F}^{\Omega}(\mathsf{k}, \mathsf{u_j})\big)$$

2. *Consider* $\overline{\Omega}$ *to be different oracles with the structure of* Ω *such that* $\overline{\Omega}$ *are consistent with* $\mathsf{L_k}$*. Sample one at random. We define* tk' *to be such that* $\mathsf{KG}^{\overline{\Omega}}(1^{\mathsf{n}}) = (\mathsf{k}, \mathsf{tk}')$*. If it does not exists* [4]*, try another one. Otherwise, we define:*
   - $\mathsf{TK_k} = \big\{(\mathsf{q}, \mathsf{i}, *) \in \mathsf{tk}' \backslash \mathsf{L_k}\big\}$
3. *We repeat this operation* $\mathsf{l_2} - 1$ *times, getting some* $\mathsf{tk_j}$*. Then:*
   - $\forall (\mathsf{q}, \mathsf{i}, *) \in \mathsf{tk_j}$*, s.t.* $(\mathsf{q}, \mathsf{i}, *) \notin \mathsf{TK_k} \cup \mathsf{L_k}$*, then* $\mathsf{TK_k} \leftarrow \mathsf{TK_k} \cup (\mathsf{q}, \mathsf{i}, \mathsf{a})$*, with* $\mathsf{a} \in_{\$} \{0,1\}^{3\mathsf{n}}$ *if* $i = 1$*,* $\mathsf{a} \in_{\$} \{0,1\}^{4\mathsf{n}}$ *if* $i = 2$*.*
4. *Now, we define* $\tilde{\Omega}_{\mathsf{k}} = \langle \tilde{\mathsf{G}}, \tilde{\mathsf{E}}, \tilde{\mathsf{D}} \rangle$*:*
   - $\tilde{\mathsf{G}}(\mathsf{sk}) = \begin{cases} \mathsf{pk} & \textit{if } (\mathsf{sk}, 1, \mathsf{pk}) \in \mathsf{TK_k} \\ \mathsf{G}_{\Omega}(\mathsf{sk}) & \textit{otherwise} \end{cases}$
   - $\tilde{\mathsf{E}}(\mathsf{pk}, \mathsf{r}, \mathsf{m}) = \begin{cases} \mathsf{a} & \textit{if } \big((\mathsf{pk}, \mathsf{r}, \mathsf{m}), 2, \mathsf{a}\big) \in \mathsf{TK_k} \\ \mathsf{E}_{\Omega}(\mathsf{pk}, \mathsf{r}, \mathsf{m}) & \textit{otherwise} \end{cases}$

     If we lose the injectivity of any $\tilde{\mathsf{E}}_{\Omega}(\mathsf{pk}, *, *)$*, we return* $\perp$*. We say that the oracle* ***jammed****.*
   - $\tilde{\mathsf{D}}(\mathsf{sk}, \mathsf{c})$*: If* $\tilde{\mathsf{E}}\big(\tilde{\mathsf{G}}(\mathsf{sk}), \mathsf{r}, \mathsf{m}\big) = \mathsf{c}$*, then* $\tilde{\mathsf{D}}(\mathsf{sk}, \mathsf{c}) = \mathsf{m}$*. Otherwise,* $\tilde{\mathsf{D}}(\mathsf{sk}, \mathsf{c}) = \perp$*.*

We can now finally define our breaker Π_M.

Definition 2.12 (Oracle Π_M)**.**
We compute $\mathsf{L_k}, \mathsf{TK_k}$*,* tk' *and thus* $\tilde{\Omega}_k$*. We define* $\mathsf{\Pi_M}(\mathsf{k}, \mathsf{y}) \to \mathsf{x}'$ *as follows:*

1. *Call* $\mathsf{T}^{\tilde{\Omega}_{\mathsf{k}}}(\mathsf{tk}', \mathsf{y}) \to \mathsf{x}'$*. Let* QT *be the list of informative queries to* $\tilde{\mathsf{D}}$ *with respect to* $\mathsf{L_k} \cup \mathsf{TK_k}$ *made by* $\mathsf{T}^{\tilde{\Omega}_{\mathsf{k}}}(\mathsf{tk}', \mathsf{y})$*.*
2. *Compute* $\mathsf{F}^{\Omega}(\mathsf{k}, \mathsf{x}') = \mathsf{z}$ *and* QFX *to be the* E*-list for* $\mathsf{F}^{\Omega}(\mathsf{k}, \mathsf{x}')$*. If* $\mathsf{z} = \mathsf{y}$ *and* $\mathsf{QT} \prec \mathsf{QTX}$*, return* x'*. Otherwise, return* $\perp$*.*

[4]Indeed, as $\mathsf{G}^{\bar{\Omega}}$ runs in n^{α}, because it is probabilistic, it can output at most $2^{n^{\alpha}}$ couple of keys, meaning that we can check all possible ones.

3 Π_M breaks $\mathsf{polyTDF}$

Let's analyse our brand new oracle. Let's first consider the jamming problem and see that it usually does not occurs.

Proposition 3.1.

$$\Pr_k\left[\tilde{\Omega}_{\mathsf{k}} \textit{ is jammed}\right] \leqslant \frac{\mathsf{l}_2\mathsf{n}^\alpha}{4^{\mathsf{n}}} + \frac{\mathsf{l}_2^2\mathsf{n}^{2\alpha}}{16^{\mathsf{n}}}$$

We define **JAM** *to be the event* $\exists k,\ \tilde{\Omega}_{\mathsf{k}}$ *is jammed.*

$$\Pr_k\left[\mathbf{JAM}\right] \leqslant \frac{\mathsf{l}_2\mathsf{n}^\alpha}{2^{\mathsf{n}}} + \frac{\mathsf{l}_2^2\mathsf{n}^{2\alpha}}{8^{\mathsf{n}}} \leqslant \mathsf{negl}(\mathsf{n})$$

meaning that jamming is a negligible problem.

Proof of Proposition 3.1:

$$\begin{aligned}
\Pr_k\left[\tilde{\Omega}_{\mathsf{k}} \text{ is jammed}\right] &\leqslant \Pr_k\left[\exists\big((\mathsf{pk},*,*),2,\mathsf{a}\big) \in \mathsf{TK}_{\mathsf{k}}, \mathsf{a} \in \mathsf{E}_\Omega(\mathsf{pk},*,*) \text{ or } \big(\mathsf{q}',2,\mathsf{a}\big) \in \mathsf{TK}_{\mathsf{k}}, \mathsf{q}' \neq (\mathsf{pk},*,*)\right] \\
&\leqslant |\mathsf{TK}_{\mathsf{k}}| \Pr_{\mathsf{a}}\left[\mathsf{a} \in \mathsf{E}_\Omega(\mathsf{pk},*,*) \cup \mathsf{TK}_{\mathsf{k}}\right] \\
&\leqslant l_2 n^\alpha \frac{4^n + l_2 n^\alpha}{16^n} \\
&\leqslant \frac{l_2 n^\alpha}{4^n} + \frac{l_2^2 n^{2\alpha}}{16^n}
\end{aligned}$$

Using union bound, we get that

$$\begin{aligned}
\Pr\left[\mathbf{JAM}\right] &= \Pr\left[\exists \mathsf{k},\ \tilde{\Omega}_{\mathsf{k}} \text{ is jammed}\right] \\
&\leqslant 2^n \Pr_k\left[\tilde{\Omega}_{\mathsf{k}} \text{ is jammed}\right] \\
&\leqslant \frac{l_2 n^\alpha}{2^n} + \frac{l_2^2 n^{2\alpha}}{8^n}
\end{aligned}$$

$\square$ 3.1

Definition 3.2 (Usual queries for F)**.**
We define the notion of ***usual queries for*** F*.*

$$\mathsf{UQ}_{\mathsf{k}}^{\mathsf{F}} = \left\{ (\mathsf{q}, \mathsf{i}, *) \;\middle|\; \Pr_{\mathsf{x}}\left[(\mathsf{q}, \mathsf{i}, *) \in \mathsf{QL}\big(\mathsf{F}^{\Omega}(\mathsf{k}, \mathsf{x})\big)\right] \geqslant \frac{1}{\epsilon_1} \right\}$$

We define $\mathbf{BAD}_1$ *to be the event* $\exists \mathsf{k},\ \mathsf{UQ}_{\mathsf{k}}^{\mathsf{F}} \nsubseteq \mathsf{L}_{\mathsf{k}}$*.*

Proposition 3.3.

$$\Pr\left[\mathsf{UQ}_{\mathsf{k}}^{\mathsf{F}} \nsubseteq \mathsf{L}_{\mathsf{k}}\right] \leqslant \epsilon_1 \mathsf{n}^{\alpha} \exp\big(-2\frac{\mathsf{l}_1}{\epsilon_1^2}\big)$$

$$\textit{Thus } \Pr\left[\mathbf{BAD}_1\right] \leqslant \epsilon_1 n^{\alpha} \exp\big(-2\frac{l_1}{\epsilon_1^2} + n\ln(2)\big)$$

Proof of Proposition 3.3:
By definition, we have that $|\mathsf{UQ}_{\mathsf{k}}^{\mathsf{F}}| \leqslant \epsilon_1 \mathsf{n}^{\alpha}$. This comes from the pigeon hall principle. We can see that all queries made by $\mathsf{F}^{\Omega}(\mathsf{k}, \mathsf{x})$ for any x as a rectangle of dimension $2^n \times n^{\alpha}$. Then, a query $\mathsf{q} \in \mathsf{UQ}_{\mathsf{k}}^{\mathsf{F}}$ must be in at least $\frac{2^n}{\epsilon_1}$ points of this rectangle. Thus,

$$\frac{2^n}{\epsilon_1}|\mathsf{UQ}_{\mathsf{k}}^{\mathsf{F}}| \leqslant 2^{\mathsf{n}}\mathsf{n}^{\alpha}$$

For all $j \in [l_1]$ and $(q, i, *) \in \mathsf{UQ}_{\mathsf{k}}^{\mathsf{F}}$, we define

$$\Delta_j^{(q,i,*)}(k) = \begin{cases} 1 & \text{if } (q, i, *) \in \mathsf{QL}\Big(\mathsf{F}^{\Omega}(\mathsf{k}, \mathsf{u_j})\Big) \\ 0 & \text{otherwise} \end{cases}$$

We have that for all $(q, i, *) \in \mathsf{UQ}_{\mathsf{k}}^{\mathsf{F}}$, $\mathbb{E}[\Delta_j^{(q,i,*)}] = \Pr[(q, i, *) \in \mathsf{QL}\big(\mathsf{F}^{\Omega}(\mathsf{k}, \mathsf{u_j})\big)] \geqslant \frac{1}{\epsilon_1}$.

Then, using Hoeffding bound, we get that

$$\begin{aligned}
\Pr\left[\mathsf{UQ}_\mathsf{k}^\mathsf{F} \nsubseteq \mathsf{L}_\mathsf{k}\right] &= \Pr\left[\exists (q,i,*) \in \mathsf{UQ}_\mathsf{k}^\mathsf{F}, \sum_{\mathsf{j}=0}^{\mathsf{l}_1} \Delta_\mathsf{j}^{(\mathsf{q},\mathsf{i},*)} = 0\right] \\
&\leqslant \left|\mathsf{UQ}_\mathsf{k}^\mathsf{F}\right| \Pr\Big[\sum_{\mathsf{j}=0}^{\mathsf{l}_1} \Delta_\mathsf{j}^{(\mathsf{q},\mathsf{i},*)} = 0\Big] \\
&\leqslant \epsilon_1 n^\alpha \Pr\Big[\sum_{j=0}^{l_1} \Delta_j - l_1 \mathbb{E}[\Delta_j] \leqslant -l_1 \mathbb{E}[\Delta_j]\Big] \\
&\leqslant \epsilon_1 n^\alpha \Pr\Big[\sum_{j=0}^{l_1} \Delta_j - l_1 \mathbb{E}[\Delta_j] \leqslant -l_1 \mathbb{E}[\Delta_j]\Big] \\
&\leqslant \epsilon_1 n^\alpha \exp\Big(-\frac{2l_1^2 \mathbb{E}[\Delta_j]^2}{l_1}\Big) \\
&\leqslant \epsilon_1 n^\alpha \exp\Big(-2\frac{l_1}{\epsilon_1^2}\Big)
\end{aligned}$$

Then, using union bound, we get that

$$\begin{aligned}
\Pr\Big[\mathbf{BAD}_1\Big] &= \Pr\Big[\exists k, \mathsf{UQ}_\mathsf{k}^\mathsf{F} \nsubseteq \mathsf{L}_\mathsf{k}\Big] \\
&\leqslant 2^n \Pr\Big[\mathsf{UQ}_\mathsf{k}^\mathsf{F} \nsubseteq \mathsf{L}_\mathsf{k}\Big] \\
&\leqslant \epsilon_1 n^\alpha \exp\big(-2\frac{l_1}{\epsilon_1^2} + n\ln(2)\big)
\end{aligned}$$

□ 3.3

Proposition 3.4.

$$\Pr\big[\mathsf{F}^\Omega(\mathsf{k},\mathsf{x}) = \mathsf{F}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{k},\mathsf{x})\big] \geqslant 1 - \epsilon_1 \mathsf{n}^\alpha \exp\big(-2\frac{\mathsf{l}_1}{\epsilon_1^2} + \mathsf{n}\ln(2)\big) - \frac{\mathsf{n}^\alpha}{\epsilon_1} - \frac{\mathsf{l}_2\mathsf{n}^\alpha}{2^\mathsf{n}} - \frac{\mathsf{l}_2^2\mathsf{n}^{2\alpha}}{8^\mathsf{n}}$$

Proof of Proposition 3.4:
See that if we are neither in $\mathbf{BAD}_1$ nor in $\mathbf{JAM}$ and that $\mathsf{QL}(\mathsf{F}^\Omega(\mathsf{k},\mathsf{x})) \subseteq \mathsf{UQ}_\mathsf{k}^\mathsf{F}$, then $\mathsf{QL}(\mathsf{F}^\Omega(\mathsf{k},\mathsf{x})) \subseteq$

$\mathsf{L_k}$ and as $\Omega\big|_{\mathsf{L_k}} = \tilde{\Omega}_\mathsf{k}\big|_{\mathsf{L_k}}$, we get, as F is deterministic, that $\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) = \mathsf{F}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{k},\mathsf{x})$. Thus,

$$\begin{aligned}\Pr_x\left[\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) = \mathsf{F}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{k},\mathsf{x})\right] &\geqslant \Pr\left[\overline{\mathbf{BAD}}_1 \wedge \overline{\mathbf{JAM}}\right] \Pr_x\left[\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) = \mathsf{F}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{k},\mathsf{x}) \middle| \mathsf{UQ}_\mathsf{k}^\mathsf{F} \subseteq \mathsf{L_k}\right] \\ &\geqslant \Pr\left[\overline{\mathbf{BAD}}_1 \wedge \overline{\mathbf{JAM}}\right] \Pr_x\left[\mathsf{QL}(\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x})) \subseteq \mathsf{UQ}_\mathsf{k}^\mathsf{F}\right]\end{aligned}$$

Now, we have to see that

$$\Pr_x\left[\mathsf{QL}(\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x})) \subseteq \mathsf{UQ}_\mathsf{k}^\mathsf{F}\right] = 1 - \Pr_\mathsf{x}\left[\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) \text{ queried } (\mathsf{q},\mathsf{i},*) \notin \mathsf{UQ}_\mathsf{k}^\mathsf{F}\right] \geqslant 1 - \frac{\mathsf{n}^\alpha}{\epsilon_1}$$

Thus,

$$\Pr_x\left[\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) = \mathsf{F}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{k},\mathsf{x})\right] \geqslant 1 - \epsilon_1 \mathsf{n}^\alpha \exp\big(-2\frac{\mathsf{l}_1}{\epsilon_1^2} + \mathsf{n}\ln(2)\big) - \frac{\mathsf{n}^\alpha}{\epsilon_1} - \frac{\mathsf{l}_2\mathsf{n}^\alpha}{2^\mathsf{n}} + \frac{\mathsf{l}_2^2\mathsf{n}^{2\alpha}}{8^\mathsf{n}}$$

□ 3.4

Corollary 3.5.

$$\Pr\left[\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{T}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{tk}',\mathsf{y})) = \mathsf{y} \;\middle|\; \mathsf{y} = \mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x})\right] \geqslant 1 - \epsilon_1\mathsf{n}^\alpha \exp(-2\frac{\mathsf{l}_1}{\epsilon_1^2}) - \frac{\mathsf{n}^\alpha}{\epsilon_1} - \frac{\mathsf{l}_2\mathsf{n}^\alpha}{2^\mathsf{n}} - \frac{\mathsf{l}_2^2\mathsf{n}^{2\alpha}}{8^\mathsf{n}}$$

Proof of Corollary 3.5:

This follows from the fact that if $\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) = \mathsf{F}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{k},\mathsf{x})$, then, as $\mathsf{T}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{tk}',\mathsf{F}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{k},\mathsf{x})) = \mathsf{x}$, we get our desired result.

□ 3.5

Proposition 3.6.
For a given $\mathsf{T}^{\tilde{\Omega}_\mathsf{k}}\big(\mathsf{k},\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x})\big)$,

$$\Pr\left[\mathsf{QT} \prec \mathsf{QFX}\right] \geqslant 1 - \frac{\mathsf{n}^\alpha 2^{2\mathsf{n}}}{2^{4\mathsf{n}} - \mathsf{n}^\alpha\mathsf{l}_1 - \mathsf{n}^\alpha\mathsf{l}_2 - 2\mathsf{n}^\alpha}$$

Proof of Proposition 3.6:
Note that with QFX, $\mathsf{L_k}$ and $\mathsf{TK_k}$, $\mathsf{T}^{\tilde{\Omega}_\mathsf{k}}$ has all the necessary information in order to retrieve x. This means that if an informative query is performed outside this field, then it is performed without any prior knowledge. Thus

$$\begin{aligned}\Pr\left[\mathsf{QT} \prec \mathsf{QFX}\right] &\leqslant n^{\alpha} \Pr\left[\mathsf{D}_{\tilde{\Omega}}(\mathsf{sk},\mathsf{c}) \neq \perp \middle| ((\mathsf{sk},\mathsf{c}),3,*) \notin \mathsf{L_k} \cup \mathsf{TK_k} \cup \mathsf{QFX} \cup \text{previous queries}\right] \\ &\leqslant n^{\alpha} \frac{2^{2n}}{2^{4n} - |\mathsf{L_k}| - |\mathsf{TK_k}| - \mathsf{QTX} - \mathsf{n}^{\alpha}} \\ &\leqslant \frac{n^{\alpha} 2^{2n}}{2^{4n} - \mathsf{n}^{\alpha}\mathsf{l}_1 - \mathsf{n}^{\alpha}\mathsf{l}_2 - 2\mathsf{n}^{\alpha}}\end{aligned}$$

□ 3.6

Corollary 3.7.
For n big-enough,

$$\mathsf{M}^{\Omega} \not\models_{\Pi_\mathsf{M}} \mathsf{polyTDF}^{\Omega,\Pi_\mathsf{M}}$$

Proof of Corollary 3.7:
We set $\epsilon_1 \geqslant n^{\alpha+2}$, $l_1 \geqslant n^{2\alpha+6}$ and $l_2 = \mathsf{poly}(\mathsf{n})$. The adversarial advantage of $\mathsf{polyTDF}^{\Omega,\Pi_\mathsf{M}}$ is

$$\mathsf{Adv}(\mathsf{A}) = \Pr\left[\mathsf{A}^{\Omega,\Pi_\mathsf{M}}(\mathsf{k},\mathsf{u}) \to \mathsf{x} \;\middle|\; \mathsf{x} \in_{\$} \{0,1\}^{\mathsf{n}}, \mathsf{KG}^{\Omega}(1^{\mathsf{n}}) \xrightarrow{\$} (\mathsf{k},\mathsf{tk}), \mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) \to \mathsf{u}\right]$$

In our case, meaning $\mathsf{A}^{\Omega,\Pi_\mathsf{M}} = \Pi_\mathsf{M}$ Using 3.1, 3.4 and 3.6, we get that

$$\begin{aligned}\mathsf{Adv}(\Pi_\mathsf{M}) &= \Pr\left[\Pi_\mathsf{M}(\mathsf{k},\mathsf{y}) \to \mathsf{x} \;\middle|\; \mathsf{x} \in_{\$} \{0,1\}^{\mathsf{n}}, \mathsf{KG}^{\Omega}(1^{\mathsf{n}}) \xrightarrow{\$} (\mathsf{k},\mathsf{tk}), \mathsf{y} = \mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x})\right] \\ &\geqslant \Pr\left[\mathsf{QT} \prec \mathsf{QFX}, \mathsf{F}^{\Omega}(\mathsf{k}, \mathsf{T}^{\tilde{\Omega}_\mathsf{k}}(\mathsf{tk}',\mathsf{y})) = \mathsf{y}, \overline{\mathbf{JAM}} \;\middle|\; \mathsf{x} \in_{\$} \{0,1\}^{\mathsf{n}}, \mathsf{KG}^{\Omega}(1^{\mathsf{n}}) \xrightarrow{\$} (\mathsf{k},\mathsf{tk}), \mathsf{y} = \mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x})\right] \\ &\geqslant 1 - \frac{n^{\alpha}2^{2n}}{2^{4n} - \mathsf{n}^{\alpha}\mathsf{l}_1 - \mathsf{n}^{\alpha}\mathsf{l}_2 - 2\mathsf{n}^{\alpha}} - \epsilon_1 n^{\alpha} \exp\big(-2\frac{l_1}{\epsilon_1^2} + n\ln(2)\big) - \frac{n^{\alpha}}{\epsilon_1} - \frac{l_2 n^{\alpha}}{2^n} - \frac{l_2^2 n^{2\alpha}}{8^n} \\ &\geqslant 1 - \frac{n^{\alpha}}{2^n} - \epsilon_1 n^{\alpha} \exp\big(-2n^2 + n\ln(2)\big) - \frac{n^{\alpha}}{n^{\alpha+2}} - \frac{l_2 n^{\alpha}}{2^n} - \frac{l_2^2 n^{2\alpha}}{8^n} \\ &\geqslant 1 - \frac{1}{n^2} - \mathsf{negl}(\mathsf{n}) \\ &\geqslant 1 - \frac{1}{n} \\ &> \mathsf{negl}(\mathsf{n})\end{aligned}$$

□ 3.7

Note that here, we consider any Π_M that can be created and it relies on the fact $\mathbf{BAD}_1$ and $\mathbf{JAM}$ do not hold.

4 Π_M does not break wPKE

Now, what remains to see is that having access Π_M does not improve significantly the adversarial capacity in attacking wPKE. To do so, we remind ourself that in 2.7, we showed that C^Ω was not only resistant to all polytime adversary, but in fact it was resistant to all computationally unbounded, poly-querying adversary.

4.1 Usual queries in tk

To do so, we have to consider what Π_M does to queries usually done by $\mathsf{KG}(1^\mathsf{n})$

Definition 4.1 (Usual queries for KG).
*We consider the **usual queries for** KG:*

$$\mathsf{UQ}_\mathsf{k}^\mathsf{KG} = \Big\{(\mathsf{q},\mathsf{i}) \;\Big|\; (\mathsf{q},\mathsf{i},*) \notin \mathsf{L}_\mathsf{k} \text{ and } \Pr_{\bar{\mathsf{tk}}}\big[(\mathsf{q},\mathsf{i},*) \in \bar{\mathsf{tk}} \;\big|\; \mathsf{KG}^{\bar\Omega}(1^\mathsf{n}) = (\mathsf{k},\bar{\mathsf{tk}})\big)\big] \geqslant \frac{1}{\epsilon_2}\Big\}$$

with $\bar\Omega$ as in the definition of $\tilde\Omega_k$ in 2.11.
We define $\mathbf{BAD}_2$ to be the event $\exists k,\ \mathsf{UQ}_\mathsf{k}^\mathsf{KG} \nsubseteq \mathsf{TK}_\mathsf{k}$.

Proposition 4.2.

$$\Pr\Big[\mathsf{UQ}_\mathsf{k}^\mathsf{KG} \nsubseteq \mathsf{TK}_\mathsf{k}\Big] \leqslant \epsilon_2 \mathsf{n}^\alpha \exp\big(-2\frac{\mathsf{l}_2}{\epsilon_2^2}\big)$$

$$\textit{Thus } \Pr\big[\mathbf{BAD}_2\big] \leqslant \epsilon_2 n^\alpha \exp\big(-2\frac{l_2}{\epsilon_2^2} + n\ln(2)\big)$$

Proof of Proposition 4.2:
By definition, we have that $|\mathsf{UQ}_\mathsf{k}^\mathsf{KG}| \leqslant \epsilon_2 \mathsf{n}^\alpha$.[5] For all $j \in [l_2]$ and $(q,i) \in \mathsf{UQ}_\mathsf{k}^\mathsf{KG}$, we define

$$\Delta_j^{(q,i)}(k) = \begin{cases} 1 & \text{if } (q,i,*) \in \mathsf{tk_j} \\ 0 & \text{otherwise.} \end{cases}$$

We have that for all $q \in \mathsf{UQ}_\mathsf{k}^\mathsf{KG}$, $\mathbb{E}[\Delta_j^q] = \Pr[(q,i,*) \in \mathsf{tk_j}] \geqslant \frac{1}{\epsilon_2}$.

[5] This is done like in the proof of 3.3

Then, using Hoeffding bound, we get that

$$\begin{aligned}
\Pr\Big[\mathsf{UQ}_\mathsf{k}^\mathsf{KG} \nsubseteq \mathsf{TK}_\mathsf{k}\Big] &= \Pr\Big[\exists (q,i) \in \mathsf{UQ}_\mathsf{k}^\mathsf{KG}, \sum_{\mathsf{j}=0}^{\mathsf{l}_2} \Delta_\mathsf{j}^{(\mathsf{q},\mathsf{i})} = 0\Big] \\
&\leqslant \big|\mathsf{UQ}_\mathsf{k}^\mathsf{KG}\big| \Pr\Big[\sum_{\mathsf{j}=0}^{\mathsf{l}_2} \Delta_\mathsf{j}^{(\mathsf{q},\mathsf{i})} = 0\Big] \\
&\leqslant \epsilon_2 n^\alpha \Pr\Big[\sum_{j=0}^{l_2} \Delta_j - l_2\mathbb{E}[\Delta_j] \leqslant -l_2\mathbb{E}[\Delta_j]\Big] \\
&\leqslant \epsilon_2 n^\alpha \Pr\Big[\sum_{j=0}^{l_2} \Delta_j - l_2\mathbb{E}[\Delta_j] \leqslant -l_2\mathbb{E}[\Delta_j]\Big] \\
&\leqslant \epsilon_2 n^\alpha \exp\Big(-\frac{2l_2^2\mathbb{E}[\Delta_j]^2}{l_2}\Big) \\
&\leqslant \epsilon_2 n^\alpha \exp\Big(-2\frac{l_2}{\epsilon_2^2}\Big)
\end{aligned}$$

Then, using union bound, we get that

$$\begin{aligned}
\Pr\Big[\mathbf{BAD}_2\Big] &= \Pr\Big[\exists k, \mathsf{UQ}_\mathsf{k}^\mathsf{KG} \nsubseteq \mathsf{TK}_\mathsf{k}\Big] \\
&\leqslant 2^n \Pr\Big[\mathsf{UQ}_\mathsf{k}^\mathsf{KG} \nsubseteq \mathsf{TK}_\mathsf{k}\Big] \\
&\leqslant \epsilon_2 n^\alpha \exp\big(-2\frac{l_2}{\epsilon_2^2} + n\ln(2)\big)
\end{aligned}$$

□ 4.2

This induce the following results.

Corollary 4.3.
For a random key k *given by* $\mathsf{G}_\Omega(1^\mathsf{n}) = (\mathsf{k}, \mathsf{tk})$*, we have that*

$$\Pr\Big[\forall(\mathsf{q},\mathsf{i},*) \in \mathsf{tk}, (\mathsf{q},\mathsf{i}) \in \mathsf{UQ}_\mathsf{k}^\mathsf{KG}\Big] \geqslant 1 - \frac{\mathsf{n}^\alpha}{\epsilon_2}$$

Furthermore, we have that

$$\Pr\Big[\exists(\mathsf{q},\mathsf{i},*) \in \mathsf{UQ}_\mathsf{k}^\mathsf{KG} \backslash \mathsf{tk}', \Omega_\mathsf{i}(\mathsf{q}) = \tilde{\Omega}_\mathsf{i}(\mathsf{q})\Big] \leqslant \frac{\mathsf{n}^\alpha \epsilon_2}{2^{3\mathsf{n}}}$$

Proof of Corollary 4.3:

$$\begin{aligned}\Pr\left[\forall(\mathsf{q},\mathsf{i},*)\in\mathsf{tk},(\mathsf{q},\mathsf{i})\in\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}\right] &= 1-\Pr\left[\exists(\mathsf{q},\mathsf{i},*)\in\mathsf{tk},(\mathsf{q},\mathsf{i})\notin\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}\right]\\ &\geqslant 1-n^{\alpha}\Pr\left[(\mathsf{q},\mathsf{i},*)\in\mathsf{tk},(\mathsf{q},\mathsf{i})\notin\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}\right]\\ &\geqslant 1-\frac{n^{\alpha}}{\epsilon_2}\end{aligned}$$

$$\begin{aligned}\Pr\left[\exists(\mathsf{q},\mathsf{i},*)\in\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}\backslash\mathsf{tk}',\Omega_{\mathsf{i}}(\mathsf{q})=\tilde{\Omega}_{\mathsf{i}}(\mathsf{q})\right] &\leqslant |\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}|\Pr\left[\Omega_{\mathsf{i}}(\mathsf{q})=\tilde{\Omega}_{\mathsf{i}}(\mathsf{q})\right]\\ &\leqslant \epsilon_2\mathsf{n}^{\alpha}\max\left\{\Pr_{\mathsf{a}}\left[\mathsf{G}_{\Omega}(\mathsf{q})=\mathsf{a}\right],\Pr_{\mathsf{a}}\left[\mathsf{E}_{\Omega}(\mathsf{q})=\mathsf{a}\right]\right\}\\ &\leqslant \epsilon_2\mathsf{n}^{\alpha}\max\left\{\frac{1}{2^{3\mathsf{n}}},\frac{1}{2^{4\mathsf{n}}}\right\}\\ &= \frac{\epsilon_2\mathsf{n}^{\alpha}}{2^{3n}}\end{aligned}$$

□ 4.3

From those results, and by merging both of them, we get the following result:

Corollary 4.4.
For any $\mathsf{c}=\mathsf{E}_{\Omega}\big(\mathsf{G}_{\Omega}(\mathsf{sk}),\mathsf{r},\mathsf{m}\big)$ *and* k *such that* $(\mathsf{sk},1,\mathsf{pk})$ *or* $\big((\mathsf{pk},\mathsf{r},\mathsf{m}),2,\mathsf{c}\big)$ *are in* tk. *Then,*

$$\Pr\left[(\mathsf{q},\mathsf{i},\Omega_{\mathsf{i}}(\mathsf{q}))\in\mathsf{QL}(\mathsf{T}^{\tilde{\Omega}_{\mathsf{k}}}(\mathsf{tk}',\mathsf{y}))\right]\leqslant\frac{\mathsf{n}^{\alpha}\epsilon_2}{2^{3\mathsf{n}}}+\frac{\mathsf{n}^{\alpha}}{\epsilon_2}$$

with $\big(\mathsf{q},\mathsf{i},\Omega_{\mathsf{i}}(\mathsf{q})\big)$ *being* $(\mathsf{sk},1,\mathsf{pk})$, $\big((\mathsf{pk},\mathsf{r},\mathsf{m}),2,\mathsf{c}\big)$ *or* $\big((\mathsf{sk},\mathsf{c}),3,\mathsf{m}\big)$.

Proof of Corollary 4.4:

$$\begin{aligned}\Pr\left[(\mathsf{q},\mathsf{i},\Omega_{\mathsf{i}}(\mathsf{q}))\in\mathsf{QL}(\mathsf{T}^{\tilde{\Omega}_{\mathsf{k}}}(\mathsf{tk}',\mathsf{y}))\right] &= \Pr\left[\big(\mathsf{q},\mathsf{i},\Omega_{\mathsf{i}}(\mathsf{q})\big)\in\mathsf{QL}\big(\mathsf{T}^{\tilde{\Omega}_{\mathsf{k}}}(\mathsf{k},\mathsf{y})\big)\ \middle|\mathsf{tk}\subseteq\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}\right]\Pr[\mathsf{tk}\subseteq\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}]\\ &+\Pr\left[\big(\mathsf{q},\mathsf{i},\Omega_{\mathsf{i}}(\mathsf{q})\big)\in\mathsf{QL}\big(\mathsf{T}^{\tilde{\Omega}_{\mathsf{k}}}(\mathsf{k},\mathsf{y})\big)\ \middle|\mathsf{tk}\nsubseteq\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}\right]\Pr[\mathsf{tk}\nsubseteq\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}]\\ &\leqslant\Pr\left[\exists(\mathsf{q},\mathsf{i},*)\in\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}\backslash\mathsf{tk}',\Omega_{\mathsf{i}}(\mathsf{q})=\tilde{\Omega}_{\mathsf{i}}(\mathsf{q})\right]+\Pr[\mathsf{tk}\nsubseteq\mathsf{UQ}_{\mathsf{k}}^{\mathsf{KG}}]\\ &\leqslant\frac{n^{\alpha}\epsilon_2}{2^{3n}}+\frac{n^{\alpha}}{\epsilon_2}\end{aligned}$$

$\square$ 4.4

We see that, if we set $\epsilon_2 \geqslant n^{\alpha+2}$ and $l_2 \geqslant n^2\epsilon_2^2 \geqslant n^{2\alpha+6}$, then this is upper bounded by $1/n$. In fact, we can make this bound as small as $1/\Theta(\mathsf{poly}(\mathsf{n}))$.
Thus, for any y, $\Pi_\mathsf{M}(\mathsf{k},\mathsf{y})$ leaks information about tk with small probability. Sadly, this probability is not negligible. We therefore require a better analysis in which we consider what occurs for queries that are not altered. This will be done by trying to simulate Π_M.

4.2 Simulating Π_M

The following results are a consequences of the fact that $\mathsf{D}_{\tilde{\Omega}}$ is fully defined by $\mathsf{G}_{\tilde{\Omega}}$ and $\mathsf{E}_{\tilde{\Omega}}$. Consider the following family

$$\mathsf{BR} = \left\{\Pi_\mathsf{M} \;\middle|\; \Pi_\mathsf{M} \text{ is a possible breaker such that } \overline{\mathbf{BAD_1}}, \overline{\mathbf{BAD}_2}, \overline{\mathbf{JAM}} \text{ holds}\right\}$$

Note that for any $\Pi_M \in \mathsf{BR}$, we have that

$$\mathsf{M}^\Omega \not\models_{\Pi_\mathsf{M}} \mathsf{polyTDF}^{\Omega,\Pi_\mathsf{M}}$$

We consider the following claim:

Claim 4.5.
Let Π_M^1 and Π_M^2 be two breakers in BR. They are indistinguishable by polynomial-time sampling.

This comes from the fact that the only case where they would differ from one another is link to the question of $\mathsf{QT} < \mathsf{QFX}$, which differ only with negligible probability. More details about this reasoning can be seen in the end of [GMM07].

This induce that given any adversary $\mathcal{A}^{\Omega,\Pi_M}$ of $\mathsf{wPKE}^{\Omega,\Pi_\mathsf{M}}$, then

$$\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi^1_\mathsf{M}}) = \mathsf{Adv}(\mathcal{A}^{\Omega,\Pi^2_\mathsf{M}}) \pm \mathsf{negl}(\mathsf{n})$$

We then split our analysis of of as follows:

$$\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}}) = \mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}}|\mathbf{INFO}) + \mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}}|\overline{\mathbf{INFO}})$$

Where **INFO** denote the fact that $\mathcal{A}^{\Omega,\Pi_M}$ performed an informative queries 2.10 using Π_M.

Let's now define a way to simulate Π_M.

Definition 4.6 (Simulation of Π_M).
We define $\Pi_{(sim)}$ a **simulation** *as follows. On call $\Pi_{(sim)}(k, y)$:*

1. *Create a $\hat{\mathsf{L}}_\mathsf{k}$ like in 2.11.*
2. *Create $\hat{\mathsf{tk}}$ and $\hat{\mathsf{TK}}_\mathsf{k}$ like in 2.11. For that, we use the fact that we are computationally unbounded and thus able to check all $\bar{\Omega}$ that are consistent with $\hat{L}_k$ and finding a $\hat{tk}$ such that $\mathsf{G}_{\bar{\Omega}}(1^\mathsf{n}) = (\mathsf{k}, \bar{\mathsf{tk}})$.*
3. *We construct $\hat{\Omega}_\mathsf{k} = \langle \hat{\mathsf{G}}, \hat{\mathsf{E}}, \hat{\mathsf{D}}_{(\mathsf{sim})} \rangle$ as follows:*
   - *$\hat{\mathsf{G}}$ is defined as $\tilde{\mathsf{G}}$ in 2.11.*
   - *$\hat{\mathsf{E}}$ is defined as $\tilde{\mathsf{E}}$ in 2.11.*
   - $\hat{\mathsf{D}}_{(\mathsf{sim})}(\mathsf{sk}, \mathsf{c}) = \begin{cases} \mathsf{m} & \textit{if } \big(\hat{\mathsf{G}}(\mathsf{sk}), \mathsf{r}, \mathsf{m}), 2, \mathsf{c}\big) \in \hat{\mathsf{TK}}_\mathsf{k} \cup \hat{\mathsf{L}}_\mathsf{k} \\ \mathsf{m} & \textit{if } \hat{\mathsf{E}}(\hat{\mathsf{G}}(\mathsf{sk}), \mathsf{r}, \mathsf{m}) = \mathsf{c} \textit{ was queried beforehand by } \mathsf{T}^{\hat{\Omega}_\mathsf{k}}(\hat{\mathsf{tk}}, \mathsf{y})^6 \\ \perp & \textit{otherwise} \end{cases}$
4. *Compute $\mathsf{T}^{\hat{\Omega}_\mathsf{k}}(\hat{\mathsf{tk}}, \mathsf{y})$ and perform the same checks than in 2.12.*

For any $\Pi_{(sim)}$, we can define a $\Pi_{(real)}$ which is defined using the same $\hat{\mathsf{L}}_\mathsf{k}, \hat{\mathsf{tk}}, \hat{\mathsf{TK}}_\mathsf{k}$ and with $\hat{\Omega}_\mathsf{k} = \langle \hat{\mathsf{G}}, \hat{\mathsf{E}}, \hat{\mathsf{D}}_{(\mathsf{real})} \rangle$, with $\hat{\mathsf{D}}_{(\mathsf{real})}$ a well defined decryption algorithm.
Note that the only point when $\Pi_{(\mathsf{sim})}(\mathsf{k}, \mathsf{y}) \neq \Pi_{(\mathsf{real})}(\mathsf{k}, \mathsf{y})$ is precisely when we require inside $\Pi_{(sim)}$ a call for $\mathsf{D}_\Omega(\mathsf{sk}', \mathsf{c}')$ such that:

- It has not been queried beforehand
- It is not in $\hat{\mathsf{TK}}_\mathsf{k} \cup \hat{\mathsf{L}}_\mathsf{k}$
- It is not $\perp$

Meaning that we are making an informative query w.r.t. $\hat{\mathsf{TK}}_\mathsf{k} \cup \hat{\mathsf{L}}_\mathsf{k}$.
Having this construction in mind, we then consider the following result.

[6] Here, there is a slight abuse of notation to simplify already heavy notations as the oracle should not be able to know such information but as it is a subroutine of an adversary, it can be done.

Lemma 4.7 (Simulating Π_M without Π_M).
For any $\mathcal{A}^{\Omega,\Pi}$ *an adversary of* $\mathsf{wPKE}^{\Omega,\Pi}$ *for* C^{Ω}*, there exists* $\mathcal{B}^{\Omega}$ *a computationally unbounded but* $\mathsf{poly(n)}$ *querying adversary of* wPKE^{Ω} *such that*

$$\mathsf{Adv}(\mathcal{B}^{\Omega}) \geqslant \mathbb{E}_{\Pi_M \in \mathsf{BR}}\Big[\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_M}|\overline{\mathbf{INFO}})\Big] - \mathsf{negl(n)}$$

Thus, using 4.5 and 2.7, we have that for any Π_M

$$\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_M}|\overline{\mathbf{INFO}}) \leqslant \mathsf{negl(n)}$$

Proof of Lemma 4.7:
We define our adversary $\mathcal{B}^{\Omega}$ as follows:

> $\mathcal{B}^{\Omega}(\mathsf{c}, \mathsf{pk}, 1^{\mathsf{n}})$:
> Create at random $\Pi_{(sim)}$.
> Run of $\mathbb{A}^{\Omega,\Pi_{(sim)}}(\mathsf{c}, \mathsf{pk}, 1^{\mathsf{n}})$.

- Note that here, create means that $\mathcal{B}^{\Omega}$ will only construct $\Pi_{(sim)}$ for the needed (queried) k (they will be only $\mathsf{poly(n)}$ many).
- We have that, as $\mathbf{BAD}_1$, $\mathbf{BAD}_2$, $\mathbf{JAM}$ don't rely on decryption, using 3.3, 3.1 and 4.2,

  $$\Pr\big[\Pi_{(real)} \text{ is such that } \overline{\mathbf{BAD}_1}, \overline{\mathbf{BAD}_2}, \overline{\mathbf{JAM}} \text{ holds }\big] \geqslant 1 - \mathsf{negl(n)}$$

  Thus, with extremely high probability, $\Pi_{(real)} \in \mathsf{BR}$.

Therefore,

$$\begin{aligned}
\mathsf{Adv}(\mathcal{B}^{\Omega}) &\geqslant \mathsf{Adv}\Big(\mathcal{B}^{\Omega}|\Pi_{(\mathsf{real})} \in \mathsf{BR}\Big)\Pr[\Pi_{(\mathsf{real})} \in \mathsf{BR}] \\
&= \sum_{\Pi \in \mathsf{BR}} \Pr[\Pi_{(real)} = \Pi]\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_{(\mathsf{sim})}})(1 - \mathsf{negl(n)}) \\
&\geqslant \sum_{\Pi \in \mathsf{BR}} \Pr[\Pi_{(real)} = \Pi]\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_{(\mathsf{real})}}|\overline{\mathbf{INFO}}) - \mathsf{negl(n)} \\
&\geqslant \mathbb{E}_{\Pi \in \mathsf{BR}}\Big[\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi}|\overline{\mathbf{INFO}})\Big] - \mathsf{negl(n)}
\end{aligned}$$

But then, using 2.7, we know that $\mathsf{Adv}(\mathcal{B}^{\Omega}) \leqslant \mathsf{negl(n)}$ and we have using 4.5 that $\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_M}|\overline{\mathbf{INFO}}) = \mathbb{E}_{\Pi \in \mathsf{BR}}\Big[\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi}_{\Pi}|\overline{\mathbf{INFO}})\Big] \pm \mathsf{negl(n)}$ inducing the last inequality.

$\square$ 4.7

This lemma thus gives us that if Π_M leads to a breach in security, it is because it performed an informative query. We now consider the following claim.

Claim 4.8.
Given pk, c*, the advantage gains from performing an informative query using* Π *and then finding* m *such that* $\mathsf{E}_\Omega(\mathsf{pk}, \mathsf{r}, \mathsf{m}) = \mathsf{c}$ *without an informative query is negligible.*

This comes from perfect secrecy and the fact, showed in 2.7, that we only gains negligible knowledge from other queries.
We can therefore assume that when an adversary $\mathcal{A}_{\Pi_\mathsf{M}}^{\Omega,\Pi_\mathsf{M}}(\mathsf{pk}, \mathsf{c}, 1^\mathsf{n})$ makes informative queries, then among those lies $\mathsf{D}_\Omega(\mathsf{sk}, \mathsf{c}) = \mathsf{m}$. This allows us to consider the following lemma.

Lemma 4.9.
For any $\mathcal{A}^{\Omega,\Pi}$ *an adversary of* $\mathsf{wPKE}^{\Omega,\Pi}$ *for* C^Ω*, we have that*

$$\mathbb{E}_{\Pi_M \in \mathsf{BR}}\Big[\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}} | \mathbf{INFO})\Big] \leqslant \mathsf{negl}(\mathsf{n})$$

Thus, using 4.5 and 2.7, we have that for any Π_M

$$\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}} | \mathbf{INFO}) \leqslant \mathsf{negl}(\mathsf{n})$$

Proof of Lemma 4.9:
This lemma comes from the following considerations. We define the oracle $\mathbf{d}$ a super decipher oracle.

$\mathbf{d}(\mathsf{sk}, \mathsf{c}, \hat{\mathsf{G}}_\mathsf{k}, \hat{\mathsf{E}}_\mathsf{k})$**:**
if $\exists \mathsf{r}, \mathsf{m}$ *s.t.* $\hat{\mathsf{E}}_\mathsf{k}(\hat{\mathsf{G}}_\mathsf{k}(\mathsf{sk}), \mathsf{r}, \mathsf{m}) = \mathsf{c}$ **then**
  return m
end
else
  return $\perp$
end

Note that, given any $\Pi_{(sim)}$, using $\mathbf{d}$, we can get $\mathsf{D}_{(\mathsf{real})}$ and thus, by replacing $\mathsf{D}_{(\mathsf{sim})}$ by $\mathsf{D}_{(\mathsf{real})}$, we get back $\Pi_{(real)}$.

Now, lets consider the following security consideration. Let $\mathcal{B}^{\Omega,\mathbf{d}}(\mathsf{c}, \mathsf{sk}, 1^\mathsf{n})$ to be any computationally unbounded but $\mathsf{poly}(\mathsf{n})$ querying whose goal is, given c, m and sk to retreave the unique r such that $\mathsf{E}_\Omega(\mathsf{G}_\Omega(\mathsf{sk}), \mathsf{r}, \mathsf{m}) = \mathsf{c}$. We have that

$$\Pr\left[\mathsf{B}^{\Omega,\mathsf{d}}(\mathsf{c},\mathsf{sk},1^{\mathsf{n}}) \to \mathsf{r} \;\middle|\; \mathsf{Gen}(1^{\mathsf{n}}) \xrightarrow{\$} (\mathsf{sk},\mathsf{pk}), \mathsf{m} \in_{\$} \{0,1\}^{\mathsf{n}}, \mathsf{r} \in_{\$} \{0,1\}^{\mathsf{n}}, \mathsf{E}_{\Omega}(\mathsf{pk},\mathsf{r},\mathsf{m}) \xrightarrow{\$} \mathsf{c}\right] \leqslant \mathsf{negl}(\mathsf{n})$$

The reasoning behind this result is quite similar to 2.7 and comes from the fact $\mathsf{c} \perp\!\!\!\perp \mathsf{r},\mathsf{m},\mathsf{sk},\mathsf{pk}$ and we gain no knowledge from some key generation G_{Ω} and any decoding $\mathbf{d}$[7]. Furthermore, on a querying $\mathsf{E}_{\Omega}(\mathsf{G}_{\Omega}(\mathsf{sk}),\mathsf{r}',\mathsf{m}) = \mathsf{c}'$:

- $\mathsf{c}' = \mathsf{c}$, but then this means that $r = r'$ and we won.
- $\mathsf{c}' \neq \mathsf{c}$, but then we only know that $r \neq r'$, which is only negligible information.

Knowing this, we now define the following adversary $\mathcal{C}^{\Omega,\mathbf{d}}(\mathsf{c},\mathsf{sk},1^{\mathsf{n}})$. It relies on the definition 2.10 which states that if Π performed an informative query but still outputs x, then those queries are among the ones performed by $\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) = \mathsf{y}$. Our adversary is defined as such:

> $\mathcal{C}^{\Omega,\mathbf{d}}(\mathsf{c},\mathsf{sk},1^{\mathsf{n}})$**:**
> Create at random $\Pi_{(sim)}$ and using $\mathbf{d}$, get $\Pi_{(real)}$.
> Simulate $A^{\Omega,\Pi_{(real)}}$ in order to retreave $\mathsf{x} = \Pi_{(\mathsf{real})}(\mathsf{k},\mathsf{y})$ such that it made $\big((\mathsf{sk},\mathsf{c}),3,\mathsf{m}\big)$ as an informative query.
> Simulate $\mathsf{F}^{\Omega}(\mathsf{k},\mathsf{x}) = \mathsf{y}$ to get $\big((\mathsf{pk},\mathsf{r},\mathsf{m}),2,\mathsf{c}\big)$.
> **return** r

Then, we simply have that

$$\begin{aligned}
\mathsf{Adv}(\mathcal{C}^{\Omega,\mathbf{d}}) &\geqslant \mathsf{Adv}\Big(\mathcal{C}^{\Omega,\mathbf{d}} | \Pi_{(\mathsf{real})} \in \mathsf{BR}\Big)\Pr[\Pi_{(\mathsf{real})} \in \mathsf{BR}] \\
&\geqslant \sum_{\Pi_M \in \mathsf{BR}} \Pr[\Pi_{(real)} = \Pi_M]\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi}|\mathbf{INFO}) - \mathsf{negl}(\mathsf{n}) \\
&= \mathbb{E}_{\Pi_M \in \mathsf{BR}}\Big[\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}}|\mathbf{INFO})\Big] - \mathsf{negl}(\mathsf{n})
\end{aligned}$$

Thus, as $\mathsf{Adv}(\mathcal{C}^{\Omega,\mathbf{d}}) \leqslant \mathsf{negl}(\mathsf{n})$ and using 4.5, we get that $\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}}|\overline{\mathbf{INFO}}) = \mathbb{E}_{\Pi_\mathsf{M} \in \mathsf{BR}}\Big[\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}}|\overline{\mathbf{INFO}})\Big] \pm \mathsf{negl}(\mathsf{n})$. Thus

$$\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_\mathsf{M}}|\mathbf{INFO}) \leqslant \mathsf{negl}(\mathsf{n})$$

□ 4.9

[7]Indeed, the decoding does not return any information about the randomness used in in encoding

Corollary 4.10.
For n big enough,

$$\mathsf{C}^{\Omega} \models \mathsf{wPKE}^{\Omega,\Pi_{\mathsf{M}}}$$

Proof of Corollary 4.10:
From 4.10 and 4.7, we get that for any $\mathcal{A}^{\Omega,\Pi_M}$ an adversary of $\mathsf{wPKE}^{\Omega,\Pi_{\mathsf{M}}}$ for C^{Ω}

$$\mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_{\mathsf{M}}}) = \mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_{\mathsf{M}}}|\mathbf{INFO}) + \mathsf{Adv}(\mathcal{A}^{\Omega,\Pi_{\mathsf{M}}}|\overline{\mathbf{INFO}}) \leqslant \mathsf{negl}(\mathsf{n})$$

which shows our desired result. □ 4.10

We therefore have, finally, proved the theorem 2.3 and thus, we have proved 2.1.

5 To go further

5.1 Extending this result to CCA PKE

We achieved to show that $\mathsf{polyTDF} \overset{\mathsf{BB}}{\not\hookrightarrow} \mathsf{PKE}$. The notion we worked during all this time, as defined in 1.5, is usually called IND-CPA PKE, because the adversaries have to distinguish between ciphertext and they can be freely encoded chosen plaintext. There exists many stronger notions of security, among those lies IND-CCA PKE.

Definition 5.1 (CCA PKE).
The primitive for IND-CCA PKE *is defined as follows :*

- $\mathsf{C}_{\mathsf{CCA\ PKE}} = \left[\lambda, \mathsf{n}, \mathsf{w}, \mathsf{Gen}, \mathsf{E}, \mathsf{D}\right]$
- $\mathsf{R}_{\mathsf{CCA\ PKE}}$ *is composed of the following requirements:*
  1. n, w *are* $\mathsf{poly}(\lambda)$.
  2. $\mathsf{Gen}, \mathsf{E}, \mathsf{D}$ *are* $\mathsf{poly}(\lambda)$.
  3. $\mathsf{Gen}(1^\lambda) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$
  4. $\mathsf{E}(\mathsf{pk}, \mathsf{m}) \xrightarrow{\$} \mathsf{c}$ *with* $\mathsf{m} \in \{0,1\}^\mathsf{n}$, $\mathsf{c} \in \{0,1\}^\mathsf{w}$.
  5. $\mathsf{D}(\mathsf{sk}, \mathsf{c}) \to \mathsf{m}$ *or* $\perp$ *with* $\mathsf{m} \in \{0,1\}^\mathsf{n}$.
  6. *Given* $\mathsf{Gen}(1^\lambda) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk})$, $\forall \mathsf{x} \in \{0,1\}^\mathsf{n}$, $\mathsf{D}\big(\mathsf{sk}, \mathsf{E}(\mathsf{pk}, \mathsf{x})\big) = \mathsf{x}$
- $\mathsf{S}_{\mathsf{CCA\ PKE}}$ *:*
  1. $\forall \mathsf{A}_1, \mathsf{A}_2\ \mathsf{PPT}(\lambda)$

$$\mathsf{Adv}(\mathsf{A}_{1,2}^{\mathsf{C},\Omega}) = \left| \Pr\left[\mathsf{A}_2^{\mathsf{C}_{\mathsf{PKE}},\Omega_{\mathsf{sk,c}}}(\mathsf{c}, \mathsf{pk}, \mathsf{m}_0, \mathsf{m}_1, \mathsf{Q}, 1^\mathsf{n}, 1^\mathsf{w}) \to \mathsf{b} \;\middle|\; \begin{array}{c} \mathsf{Gen}(1^\lambda) \xrightarrow{\$} (\mathsf{sk}, \mathsf{pk}), \mathsf{b} \in_{\$} \{0,1\}, \\ \mathsf{A}_1^{\mathsf{C}_{\mathsf{PKE}},\Omega_{\mathsf{sk,c}}}(\mathsf{pk}, 1^\mathsf{n}, 1^\mathsf{w}) \xrightarrow{\$} (\mathsf{m}_0, \mathsf{m}_1, \mathsf{Q}), \mathsf{E}(\mathsf{pk}, \mathsf{m}_\mathsf{b}) \xrightarrow{\$} \mathsf{c} \end{array} \right] - \frac{1}{2} \right| \leqslant \mathsf{negl}(\lambda)$$

With $\Omega_{\mathsf{sk,c}}$ *an oracle such that* $\Omega_{\mathsf{sk,c}}(\mathsf{x})$

- *If* $\mathsf{x} = \mathsf{c}$, *return* $\perp$
- *else, return* $\mathsf{D}(\mathsf{sk}, \mathsf{x})$

We easily see that $\mathsf{PKE} \overset{\mathsf{BB}}{\hookrightarrow} \mathsf{CCA\ PKE}$. A very good question is therefore to know if 2.1 extend to IND-CCA PKE ? We cannot answer either by the positive nor the negative and this question is in active research and can be attack in two ways:

- Head on, and some interesting results can be found in [KMT22].
- Try to find, similarly to 1.14, as way to find $\mathsf{CCA\ PKE} \overset{\mathsf{BB}}{\hookrightarrow} \mathsf{PKE}$. This is an active research question. All of the known only known blackbox constructions ([HHK17]) are based on the

Fujisaki-Okamoto transform [FO13] whose analysis is done in the random oracle model. The problem is that this does not help us in this problem. Indeed, [BHSV98] showed that $\mathsf{polyTDF} \xhookrightarrow[\mathsf{ROM}]{\mathsf{BB}} \mathsf{CCA\ PKE}$.

- Furthermore, using the second option might not be useful as they might be a separation between CCA PKE and PKE. Indeed, in [GMM07], the authors of the original paper reused the tools we used in order to perform an almost separation between CCA1 PKE and PKE.[8] More precisely, they showed they were no blackbox reduction of CCA1 PKE into PKE of the form

$$\mathsf{M}^{\mathsf{g,e,d}} = \langle \mathsf{Gen}^{\mathsf{g,e,d}}_{\mathsf{CCA1}}, \mathsf{E}^{\mathsf{g,e,d}}_{\mathsf{CCA1}}, \mathsf{D}^{\mathsf{g,d}}_{\mathsf{CCA1}} \rangle$$

5.2 To sum up

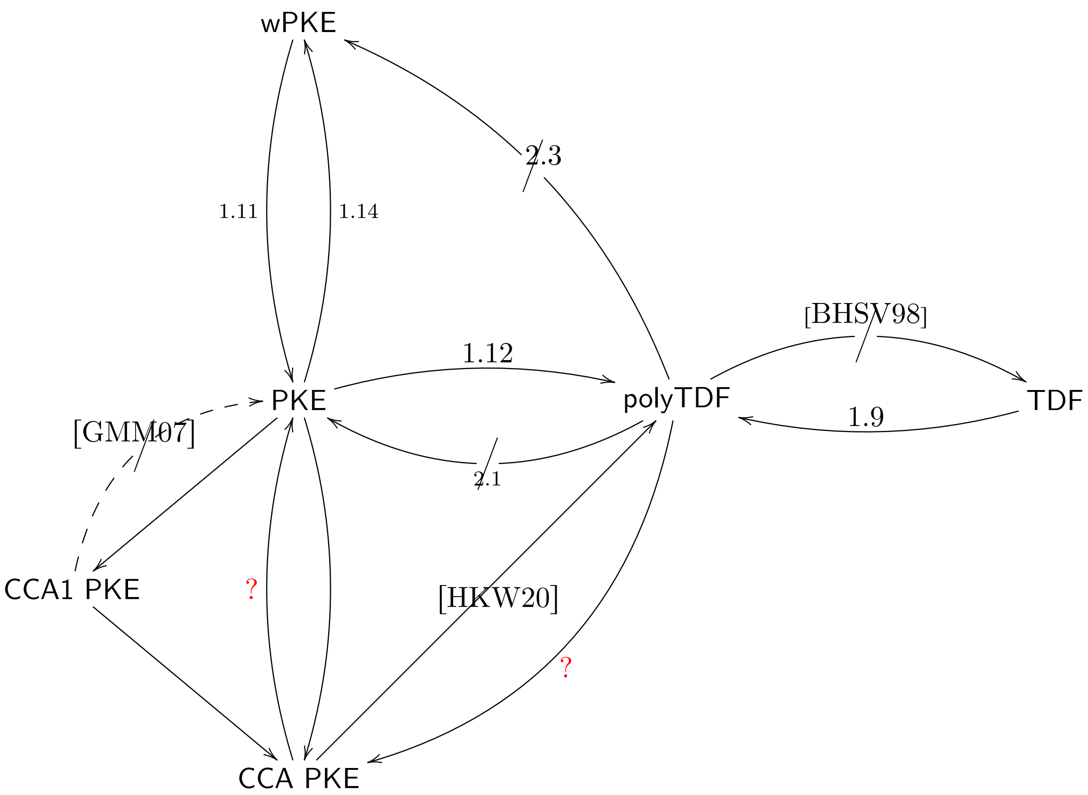

Figure 1: Discussed blackbox separation diagram

Note that, in some of the literature, this diagram is shown reverse, as the arrows $A \to B$ describe the fact that having A induce having B.

[8] CCA1 PKE denote the weaker primitive derived from CCA PKE where only A_1 has access to $\Omega_{sk,c}$.

Acknowledgement

I would like to give the biggest thanks possible to the following people:

- To Loïs Huguenin-Dumittan, whose unending support, quick thinking and illuminating indications made this project what it is today. He was always there for me and I cannot thank him enough.
- To Serge Vaudenay, for giving me the opportunity to work on this subject in the LASEC.
- To Yael Gertner, Tal Malkin and Omer Reingold and many others for their work from whom this paper is only a low degree extention.

References

[BBF13] Paul Baecher, Christina Brzuska, and Marc Fischlin, *Notions of black-box reductions, revisited*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2013, pp. 296–315.

[BHSV98] Mihir Bellare, Shai Halevi, Amit Sahai, and Salil Vadhan, *Many-to-one trapdoor functions and their relation to public-key cryptosystems*, Annual International Cryptology Conference, Springer, 1998, pp. 283–298.

[BN13] Ahto Buldas and Margus Niitsoo, *Black-box separations and their adaptability to the non-uniform model*, Australasian Conference on Information Security and Privacy, Springer, 2013, pp. 152–167.

[DH76] Whitfield Diffie and Martin E Hellman, *New directions in cryptography*, Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, 1976, pp. 365–390.

[DOP05] Yevgeniy Dodis, Roberto Oliveira, and Krzysztof Pietrzak, *On the generic insecurity of the full domain hash*, Annual International Cryptology Conference, Springer, 2005, pp. 449–466.

[Fis12] Marc Fischlin, *Black-box reductions and separations in cryptography*, International Conference on Cryptology in Africa, Springer, 2012, pp. 413–422.

[FLR$^+$10] Marc Fischlin, Anja Lehmann, Thomas Ristenpart, Thomas Shrimpton, Martijn Stam, and Stefano Tessaro, *Random oracles with (out) programmability*, International Conference on the Theory and Application of Cryptology and Information Security, Springer, 2010, pp. 303–320.

[FO13] Eiichiro Fujisaki and Tatsuaki Okamoto, *Secure integration of asymmetric and symmetric encryption schemes*, Journal of cryptology **26** (2013), no. 1, 80–101.

[FS12] Dario Fiore and Dominique Schröder, *Uniqueness is a different story: Impossibility of verifiable random functions from trapdoor permutations*, Theory of Cryptography Conference, Springer, 2012, pp. 636–653.

[GGH19] Sanjam Garg, Romain Gay, and Mohammad Hajiabadi, *New techniques for efficient trapdoor functions and applications*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2019, pp. 33–63.

[GL89] Oded Goldreich and Leonid A Levin, *A hard-core predicate for all one-way functions*, Proceedings of the twenty-first annual ACM symposium on Theory of computing, 1989, pp. 25–32.

[GM82] Shafi Goldwasser and Silvio Micali, *Probabilistic encryption & how to play mental poker keeping secret all partial information*, Proceedings of the fourteenth annual ACM symposium on Theory of computing, 1982, pp. 365–377.

[GMM07] Yael Gertner, Tal Malkin, and Steven Myers, *Towards a separation of semantic and cca security for public key encryption*, Theory of Cryptography Conference, Springer, 2007, pp. 434–455.

[GMR01] Yael Gertner, Tal Malkin, and Omer Reingold, *On the impossibility of basing trapdoor functions on trapdoor predicates*, Proceedings 42nd IEEE Symposium on Foundations of Computer Science, IEEE, 2001, pp. 126–135.

[HHK17] Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz, *A modular analysis of the fujisaki-okamoto transformation*, Theory of Cryptography Conference, Springer, 2017, pp. 341–371.

[HJKS10] Kristiyan Haralambiev, Tibor Jager, Eike Kiltz, and Victor Shoup, *Simple and efficient public-key encryption from computational diffie-hellman in the standard model*, International Workshop on Public Key Cryptography, Springer, 2010, pp. 1–18.

[HKW20] Susan Hohenberger, Venkata Koppula, and Brent Waters, *Chosen ciphertext security from injective trapdoor functions*, Annual International Cryptology Conference, Springer, 2020, pp. 836–866.

[HR04] Chun-Yuan Hsiao and Leonid Reyzin, *Finding collisions on a public road, or do secure hash functions need secret coins?*, Annual International Cryptology Conference, Springer, 2004, pp. 92–105.

[IR89] Russell Impagliazzo and Steven Rudich, *Limits on the provable consequences of one-way permutations*, Proceedings of the twenty-first annual ACM symposium on Theory of computing, 1989, pp. 44–61.

[KMT22] Fuyuki Kitagawa, Takahiro Matsuda, and Keisuke Tanaka, *Cca security and trapdoor functions via key-dependent-message security*, Journal of Cryptology **35** (2022), no. 2, 1–69.

[RTV04] Omer Reingold, Luca Trevisan, and Salil Vadhan, *Notions of reducibility between cryptographic primitives*, Theory of Cryptography Conference, Springer, 2004, pp. 1–20.

[Sim98] Daniel R Simon, *Finding collisions on a one-way street: Can secure hash functions be based on general assumptions?*, International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1998, pp. 334–345.

[Yao82] Andrew C Yao, *Theory and application of trapdoor functions*, 23rd Annual Symposium on Foundations of Computer Science (SFCS 1982), IEEE, 1982, pp. 80–91.