Composing Bridges

Mugurel Barcau[1,2], Vicenţiu Paşol[1,2], and George C. Ţurcaş[1,3]

[1] certSIGN – Research and Innovation, Bucharest, Romania
[2] Institute of Mathematics "Simion Stoilow" of the Romanian Academy
[3] Babeş-Bolyai University, Cluj-Napoca, Romania
{alexandru.barcau,vicentiu.pasol,george.turcas}@certsign.ro

Abstract. The present work builds on previous investigations of the authors (and their collaborators) regarding bridges, a certain type of morphisms between encryption schemes, making a step forward in developing a (category theory) language for studying relations between encryption schemes. Here we analyse the conditions under which bridges can be performed sequentially, formalizing the notion of composability. One of our results gives a sufficient condition for a pair of bridges to be composable. We illustrate that composing two bridges, each independently satisfying a previously established IND-CPA security definition, can actually lead to an insecure bridge. Our main result gives a sufficient condition that a pair of secure composable bridges should satisfy in order for their composition to be a secure bridge. We also introduce the concept of a *complete* bridge and show that it is connected to the notion of Fully composable Homomorphic Encryption (FcHE), recently considered by Micciancio. Moreover, we show that a result of Micciancio which gives a construction of FcHE schemes can be phrased in the language of complete bridges, where his insights can be formalised in a greater generality.

Keywords: Bridge · Composability · Fully Composable Homomorphic Encryption · IND-CPA security

1 Introduction

1.1 When designing a complex cryptographic solution, one has to combine multiple cryptographic protocols and the interaction between these protocols is playing an important role in the security of the global solution. For example, in such a solution one might have ciphertexts encrypted under different secret keys, or even encrypted using different encryption schemes. This gives rise to the necessity of switching ciphertexts encrypted using one secret key to ciphertexts encrypted under a different key. A solution can be found in the literature under the name of Proxy Re-Encryption (see [8] and the references within). A similar idea emerges in Hybrid Homomorphic Encryption (see for example [17] and [18]). Such a protocol is used mainly to reduce bandwidth costs resulting from ciphertext expansion for the homomorphic encryption schemes. When Hybrid Homomorphic Encryption is deployed, a server is able to convert ciphertexts

encrypted using a symmetric cipher to ciphertexts encrypted using a homomorphic encryption scheme. In our previous work [3], we defined and gave examples of *bridges*, formalizing the conditions under which an algorithm that publicly transforms encrypted data from one scheme to another should perform. In the same work, we defined the IND-CPA security of a bridge by relating it to the security of a specific encryption scheme associated to the bridge.

1.2 Here we take a step forward and study the context of interactions between bridges and deal with their security from a global point of view in relation with their individual security considerations. For a fair general treatment of this situation, we point out to the work of Canetti and his collaborators ([10],[11],[12]). In this work we are concerned with the sequential evaluation, i.e. composition, of multiple bridges. Ideally, after composing two bridges, the resulting ciphertext should preserve the underlying plaintext after decryption. The notion of composability we use and define here for bridges is finer than the mere instantiation to our case of the universal composition (UC) notion of Canetti. The universality UC theorem does not apply in our setting, and neither do the modularity results that can be deduced from the aforementioned theorem. In our Example 4, both components (protocols) are secure, while their composition fails this requirement. Moreover, the correctness property (which is seen in the ideal-process framework as a security feature) also fails for the generic composition of bridges. However, we remark that our main theorems which give sufficient conditions for the composition of bridges to be correct and secure resemble the ideal-process structural shape in the work of Canetti [10], namely, the indistinguishability from a process that can be (publicly) described.

1.3 Let us recall some practical and theoretical applications of bridges. Proxy Re-Encryption can be used in protocols for secure distribution of files [1], e-mail forwarding and secure payments. As pointed out in [9, page 2], a procedure called "key rotation", based on Proxy Re-Encryption is required by Payment Card Industry Data Security Standard (PCI DSS) and by the Open Web Application Security Project (OWASP).

In practice, by construction, all Proxy Re-Encryption (PRE) protocols can convert ciphertexts between the same scheme. Recently, the theoretical concept of Universal Proxy Re-Encryption (UPRE) [19] was proposed in order to extend the concept of PRE by accommodating scenarios in which a delegate can convert ciphertexts from a PKE scheme into ciphertexts of a potentially different PKE scheme. Unfortunately, UPREs are very difficult to realize in practice.

The overwhelming majority of the examples discussed here involve Fully Homomorphic Encryption (FHE) schemes. Within this setting, *bootstrapping* procedures (such as the recent bootstrapping in FHEW-like cryptosystems [28,26]) are of great importance. As we pointed out in [3], these give rise to bridges. The theoretical language of bridges developed in the present work offers a conceptual framework for explaining the following previously known fact about certain homomorphic encryption schemes: if one performs a circuit on encrypted data (which is a bridge) and then a bootstrapping procedure (which is also a bridge), then the correctness of decryption is preserved (hence one obtains a third bridge).

In the previous situation, the IND-CPA security analysis of the third bridge reduces to the *circular security* of the homomorphic encryption scheme.

1.4 The present article is a natural continuation of the work in [3], where the underlying motivation was to create a category whose objects are encryption schemes, aiming to understand relations among them. Considering bridges as viable candidates for the arrows in such a category, one is naturally lead to the notion of composing bridges. As we mention in Remark 4 bellow, one can perform composition of bridges when restricting to bridges that are *complete*. Unfortunately, composition is not compatible with yet another feature of encryption schemes, namely their semantic security. Thus, we are forced, for the moment, to further restrict the morphisms in our envisaged category to *Gentry-type* bridges as Theorem 4 asserts. Sadly, this constraint on morphisms forces a restriction on the objects (i.e. encryption schemes), namely in this setting one must restrict to the study of relations between FHE schemes. Moreover, if we want to allow "self-morphisms" (there is a nuance that differentiates them from endomorphisms), i.e. bridges between the same scheme which have the *same* secret key, then we need to limit our attention to those FHE schemes which are circular secure (see Theorem 5).

1.5 As we shall see throughout this paper, multiple technical difficulties arise when one sequentially performs bridges.

Firstly, as we point out shortly after Definition 7, due to the possible loss of correctness of decryption, the composition of two bridges is not necessarily a bridge. We overcome this by introducing the notion of *complete bridges* (see Definition 8), a type of bridge which satisfies an enhanced correctness property with respect to the decryption algorithms. We then show (in Proposition 1) that complete bridges can be composed.

Secondly, in Section 5 we observe that, even if one is able to compose two *secure bridges*, the resulting bridge might not be secure (see Example 4). Theorem 2 gives a sufficient condition on a pair of composable secure bridges for their composition to be secure.

1.6 We apply our theoretical results to certain types of bridges that arise in the context of homomorphic encryption schemes. In such schemes, some boolean circuits can be evaluated on encrypted data and such an evaluation is called homomorphic. We show that the homomorphic evaluation of a circuit gives rise to a bridge between a *fiber power* of the encryption scheme to the scheme itself (see Section 7).

In a recent talk, Micciancio [27] points out that the definition of fully homomorphic encryption does not guarantee that one can sequentially homomorphically evaluate two circuits while preserving correct decryption. In this paper, we formulate the previous aspect in the language of bridges. The mere definition of a correct bridge does not guarantee that one can further apply another bridge to the resulting ciphertext of the first bridge without the risk of loosing correctness. Motivated by the definitional issue raised above, Micciancio introduces the notion of fully composable homomorphic encryption (FcHE) and inspired by

the bootstrapping procedure (used to construct FHE schemes) he sketches [27] the proof of a theorem asserting sufficient conditions for the existence of a FcHE scheme. The security of the FcHE scheme constructed by Micciancio follows from the circular security of a FHE. To address an analogous issue, building up on previous work in [3], we introduce the definition of a *complete* bridge. Finally, we show that the aforementioned result of Micciancio [27] can be phrased in the language of bridges, where its proof becomes more conceptual. In our proof, we constructed a special type of bridge inspired from the *Gentry type* bridges defined in [3]. The difference between the former and later bridges is subtle and resides in their KeyGen algorithms. The KeyGen algorithm for the bridge needed in this proof satisfies an additional condition which accounts for the fact that the security of this bridge is equivalent to the circular security of a homomorphic encryption scheme.

1.7 The paper is organized as follows. In the next section we give some preliminaries used throughout the paper. In Section 3 we recall the main concepts needed in this article. We define complete and composable bridges in Section 4 and prove that complete bridges are composable. In Section 5 we investigate the security of composition of bridges and prove our main result. The next section is dedicated to Gentry-type bridges and compositions of general bridges with such bridges, proving the correctness and security of these protocols. In the last section, we explicitly construct bridges from circuits and show how one can translate the original discussion of Micciancio about composition of homomorphic evaluation of circuits into our language of bridge composition.

1.8 In his talk, Micciancio explained that one of the motivations of his analysis was the connection between circular security and fully composable homomorphic encryption. The biggest hope is to place circular security into a larger setting, which will then allow to possibly prove that circular security reduces to standard assumptions. We are informally asking if the language of bridges and bridge composition adds valuable insights into this problem. In addition, the theory of composable bridges can be related to the way the third generation of FHE schemes realise the bootstrapping procedure. Indeed, the accumulator proposed in [20] can be viewed as a composition of bridges, one of which is a Gentry type bridge. It would be interesting to further investigate the connections between this theory and the theory of fully homomorphic encryption schemes constructed on the LWE assumption.

Acknowledgements

The authors are indebted to George Gugulea, Cristian Lupaşcu and Mihai Togan for helpful discussions and comments during the preparation of this work.

2 Preliminaries

In all our definitions, we denote the security parameter by λ. We say that a function $\mathrm{negl} : \mathbb{N} \to [0, +\infty)$ is a negligible function if for any positive integer c there exists a positive integer N_c, such that $\mathrm{negl}(n) < \frac{1}{n^c}$ for all $n \geq N_c$.

Throughout this article, we will use the language of finite distributions (see section 2.1 of [3]). In particular, an encryption scheme comes with the following finite distributions: secret keys, public keys and the encryptions of every fixed message. To be precise, all of the distributions mentioned here are defined for each fixed value of the security parameter λ. For example, the secret key distributions $\{\mathcal{SK}_\lambda : \lambda \in \mathbb{N}\}$ form an ensemble of finite distributions. Such ensembles form a category, in which one can define finite products and study relations between its objects. To fix ideas, we choose to recall the following illustrative example of a relation between two finite distributions. Given λ, the key generation algorithm of an encryption scheme gives rise to the distribution of secret keys $\mathcal{SK}_\lambda$ and, for each sample $sk \leftarrow \mathcal{SK}_\lambda$, the second part of the algorithm outputs a sample pk from a distribution of public keys. We say that the resulted distribution of public keys $\mathcal{PK}_\lambda$ is an $\mathcal{SK}_\lambda$-distribution. More details about the language of finite distributions and the relations between the distributions associated to an encryption scheme are explained in [3].

In an effort to keep the notation simple, we sometimes omit the subscript λ when referring to a certain ensemble of finite distributions. We will use upper case calligraphic letters for the name of the distributions and lower case italic letters for samples from various distributions.

Every PPT algorithm gives rise to a probability distribution. Throughout this work, every written identity that involves the output of a PPT algorithm is assumed to hold with overwhelming probability over the randomness introduced by the PPT algorithm. This means that the probability of failure of that identity is negligible. For brevity, we shall avoid the repeated use of the phrase "with overwhelming probability" to indicate this situations.

3 Definitions

We first recall two technical definitions about ensembles of finite distributions discussed in more detail in [3].

Definition 1. *An ensemble $\{\mathcal{X}_\lambda\}_\lambda$ of finite distributions is polynomial-time constructible if there exists a PPT algorithm A such that $A(1^\lambda) = \mathcal{X}_\lambda$, for every λ. An $\{\mathcal{X}_\lambda\}_\lambda$-ensemble of finite distributions $\{(\mathcal{Y}_\lambda, \varphi_\lambda : \mathcal{Y}_\lambda \to \mathcal{X}_\lambda)\}_\lambda$ is polynomial-time constructible on fibers if there exist a PPT algorithm A, such that for any $x_\lambda \leftarrow \mathcal{X}_\lambda$ we have $A(1^\lambda, x_\lambda) = \mathcal{Y}_\lambda|_{\mathcal{X}_\lambda = x_\lambda}$, where $\mathcal{Y}_\lambda|_{\mathcal{X}_\lambda = x_\lambda}$ is the fiber distribution over x_λ.*

We will also use the following notion of computational (or polynomial) indistinguishability from [25] and [24].

Definition 2. *Two ensembles of finite distributions* $\{\mathcal{X}_\lambda\}_\lambda$ *and* $\{\mathcal{Y}_\lambda\}_\lambda$ *are called computationally indistinguishable if for any PPT distinguisher* D*, the quantity*

$$|\Pr\{D(\mathcal{X}_\lambda) = 1\} - \Pr\{D(\mathcal{Y}_\lambda) = 1\}|$$

is negligible as a function of λ*.*

Next, we review some notions related to public key encryption schemes, homomorphic encryption and bridges between encryption schemes.

Definition 3 (PKE). *A public key encryption scheme consists of three PPT algorithms*

$$\mathcal{E} = (\text{KeyGen}, \text{Enc}, \text{Dec})$$

as follows:

- KeyGen: *The algorithm* $(sk, pk) \leftarrow \text{KeyGen}(1^\lambda)$ *takes a unary representation of the security parameter and outputs a secret key* sk *and a public key* pk*.*
- Enc: *The algorithm* $c \leftarrow \text{Enc}(pk, m)$ *takes the public key* pk *and a single message* $m \in \mathcal{M}$ *and outputs a ciphertext* $c \in \mathcal{C}$*.*
- Dec: *The algorithm* $m^* \leftarrow \text{Dec}(sk, c)$ *takes the secret key* sk *and a ciphertext* c *and outputs a message* m^**.*

We shall always assume that a public key encryption scheme is *correct*, i.e. it satisfies the following property:
Correct Decryption: The scheme $\mathcal{E}$ is correct if for all $m \in \mathcal{M}$ and all pairs of keys (sk, pk) outputted by $\text{KeyGen}(1^\lambda)$,

$$\text{Dec}(sk, \text{Enc}(pk, m)) = m,$$

with overwhelming probability over the finite distribution $\text{Enc}(pk, m)$.

A (public key) homomorphic encryption scheme is a PKE scheme such that its KeyGen algorithm outputs an additional evaluation key evk (besides sk and pk), which is used by an additional PPT evaluation algorithm Eval. To be precise, there is a fourth PPT algorithm:

- Eval: The algorithm takes the evaluation key evk, a representation of a boolean circuit $C : \mathcal{M}^\ell \to \mathcal{M}$ from a set of evaluable circuits $\mathcal{L}$, and a set of ℓ ciphertexts $c_1, ..., c_\ell$, and outputs a ciphertext $c^* \leftarrow \text{Eval}(evk, C, c_1, \ldots, c_\ell)$.

Relative to the evaluation algorithm, a public-key homomorphic encryption scheme is assumed to satisfy the following correctness property:
Correct Evaluation: The scheme $\mathcal{E}$ correctly evaluates all boolean circuits in $\mathcal{L}$ if for all keys (sk, pk, evk) outputted by $\text{KeyGen}(1^\lambda)$, for all circuits $C : \mathcal{M}^\ell \to \mathcal{M}$, $C \in \mathcal{L}$, and for all $m_i \in \mathcal{M}$, $1 \leq i \leq \ell$, it holds that

$$\text{Dec}(sk, \text{Eval}(evk, C, \text{Enc}(pk, m_1), ..., \text{Enc}(pk, m_\ell)) = C(m_1, ..., m_\ell),$$

with overwhelming probability over the randomness of Enc and Eval.

Remark. Nowadays, although omitted from most definitions, it is understood that all homomorphic encryptions schemes should satisfy a certain compactness property, namely that there exists a polynomial $s = s(\lambda)$ such that the output length of Eval is at most s bits long, regardless of $C \in \mathcal{L}$ or the number of inputs.

We say that a public-key homomorphic encryption scheme is a *fully homomorphic encryption (FHE) scheme (over $\mathcal{M}$)* if the scheme correctly evaluates all possible boolean circuits $C : \mathcal{M}^\ell \to \mathcal{M}$, for $\ell \in \mathbb{N}$.

The authors of [3] proposed a general definition for an algorithm that publicly transforms encrypted data from one scheme to another. We recall here their definition of a *bridge* between two encryption schemes.

Definition 4. *Let $\mathcal{E}_i = (\mathrm{KeyGen}_i, \mathrm{Enc}_i, \mathrm{Dec}_i)$, $i \in \{1, 2\}$ be two PKE schemes. A bridge $\mathbf{B}_{\iota,f}$ from $\mathcal{E}_1$ to $\mathcal{E}_2$ consists of:*

1. *A function $\iota : \mathcal{M}_1 \to \mathcal{M}_2$ that is computable by a deterministic polynomial time algorithm, where $\mathcal{M}_i$ is the plaintext space of the scheme $\mathcal{E}_i$.*
2. *A PPT bridge key generation algorithm, which has the following three stages. First, the algorithm gets the security parameter λ and uses it to run KeyGen_1 in order to obtain a pair of keys sk_1, pk_1. In the second stage the algorithm uses sk_1 to find a secret key sk_2 of level λ for $\mathcal{E}_2$, and then uses the second part of KeyGen_2 to produce pk_2. In the final stage, the algorithm takes as input the quadruple (sk_1, pk_1, sk_2, pk_2) and outputs a bridge key bk.*
3. *A PPT algorithm f which takes as input the bridge key bk and a ciphertext $c_1 \in \mathscr{C}_1$ and outputs a ciphertext $c_2 \in \mathscr{C}_2$, such that*

$$\mathrm{Dec}_2(sk_2, f(bk, \mathrm{Enc}_1(pk_1, m))) = \iota(m).$$

Remark. To simplify the discussion, when $\iota : \mathcal{M}_1 \to \mathcal{M}_2$ is clear from the context, we will abuse notation and write $f : \mathcal{E}_1 \to \mathcal{E}_2$ instead of the bridge $\mathbf{B}_{\iota,f}$.

We now give the definition/construction of the k-th fiber power encryption scheme $\mathcal{E}^{(k)}$, associated to any encryption scheme $\mathcal{E}$ and any positive integer k.

Definition 5. *Let $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ be a PKE scheme, such that $\mathcal{M}$ and $\mathcal{C}$ are its plaintext and ciphertext spaces. For any positive integer k, the k-th fiber power of $\mathcal{E}$ is the encryption scheme $\mathcal{E}^{(k)} = (\mathrm{KeyGen}, \mathrm{Enc}^{(k)}, \mathrm{Dec}^{(k)})$, whose plaintext and ciphertext are the k-th Cartesian products $\mathcal{M}^k$ and $\mathcal{C}^k$ respectively. Moreover, the key generation algorithm is identical to the one of $\mathcal{E}$, outputting a pair (sk, pk). The encryption and decryption algorithms of $\mathcal{E}^{(k)}$ are*

$$\mathrm{Enc}^{(k)}(pk, (m_1, \ldots, m_k)) = (\mathrm{Enc}(pk, m_1), \ldots, \mathrm{Enc}(pk, m_k))$$

and

$$\mathrm{Dec}^{(k)}(sk, (c_1, \ldots, c_k)) = (\mathrm{Dec}(sk, c_1), \ldots, \mathrm{Dec}(sk, c_k)),$$

for any $(m_1, \ldots, m_k) \in \mathcal{M}^k$ and $(c_1, \ldots, c_k) \in \mathcal{C}^k$.

Remark 1. In the category $\mathscr{F}in\mathscr{D}ist$ of finite distributions, the encryptions of the defined scheme $\mathcal{E}^{(k)}$ are products of k copies of the distributions of encryptions from $\mathcal{E}$ regarded as $\mathcal{PK}$- distributions, as defined in Section 2.1 of [3].

We end this section with a simple example of a bridge from $\mathcal{E}^{(2)}$ to $\mathcal{E}$, whose importance will become apparent in the next section. Moreover, construction of certain bridges from $\mathcal{E}^{(k)}$ to $\mathcal{E}$, for general k, will play a crucial role in our work presented here.

Example 1. We recall briefly the definition of a basic homomorphic LWE encryption scheme with plaintext space $\mathcal{M} = \mathbb{Z}_2$. The scheme $\mathcal{E}$ is parameterized by a dimension n, a ciphertext modulus $q = n^{O(1)}$ and a randomized rounding function $\chi : \mathbb{R} \to \mathbb{Z}$. In order to achieve an additive homomorphic property, we impose that the rounding function has error distribution satisfying $|\chi(x) - x| < q/8$. The secret key of the encryption scheme is a vector $sk \in \mathbb{Z}_q^n$, which is chosen uniformly at random. For simplicity, we will assume that this scheme is symmetric, namely that the public key $pk = sk$. The encryption of a message $m \in \mathbb{Z}_2$ under the key $sk \in \mathbb{Z}_q^n$ is given by

$$\mathrm{Enc}(pk, m) = (a, \chi(a \cdot sk + mq/2) \bmod q) \in \mathbb{Z}_q^{n+1},$$

where $a \leftarrow \mathbb{Z}_q^n$ is chosen uniformly at random. A ciphertext (a, b) is decrypted as follows

$$\mathrm{Dec}(sk, (a, b)) = \lfloor 2(b - a \cdot sk)/q \rceil \bmod 2.$$

Note that correction of the decryption follows from the assumption on the rounding error of χ. Using the homomorphic addition that can be performed on this scheme, we can easily construct a bridge from $\mathcal{E}^{(2)}$ to $\mathcal{E}$, as we now explain.

The function $\iota : \mathcal{M} \times \mathcal{M} \to \mathcal{M}$ is defined as $\iota(m_1, m_2) = m_1 + m_2$, where the addition is performed in $\mathbb{Z}_2$.

The key generation algorithm of the bridge uses the key generation algorithm of $\mathcal{E}^{(2)}$ to output a pair (sk, pk) and then, in the second stage, associates the same pair (sk, pk) to $\mathcal{E}$. Finally, the algorithm outputs an empty bridge key bk.

The ppt algorithm f takes a pair of ciphertexts $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}_q^{n+1}$ and computes

$$f((a_1, b_1), (a_2, b_2)) := (a_1 + a_2, b_1 + b_2).$$

The correctness property of the bridge follows immediately from the fact that the rounding error of χ is less than $q/8$, in other words the corectness is implied by the additive homomorphic property of the scheme $\mathcal{E}$.

Remark 2. Note that in the setting above, given a pair of elements in the ciphertext space $(a_1, b_1), (a_2, b_2) \in \mathbb{Z}_q^{n+1}$, it is not true in general that

$$\mathrm{Dec}(sk, f((a_1, b_1), (a_2, b_2))) = \mathrm{Dec}(sk, (a_1, b_1)) + \mathrm{Dec}(sk, (a_2, b_2)).$$

To see this, if $\mathrm{Dec}(sk, (a_i, b_i)) = m_i$, then the error $b_i - a_i \cdot s_k - m_i q/2 \bmod q$ might not lie in the interval $(-q/8, q/8)$, for some $i \in \{1, 2\}$. In this case, $b_1 +$

$b_2 - (a_1 + a_2) \cdot sk - (m_1 + m_2)q/2 \bmod q$ might not belong to $(-q/4, q/4)$, so that

$$\mathrm{Dec}(sk, f((a_1, b_1), (a_2, b_2))) = \mathrm{Dec}(sk, (a_1 + a_2, b_1 + b_2))$$

is not guaranteed to be equal to $m_1 + m_2$.

4 Complete and composable bridges

In general, as we noticed in the last remark of the previous section, the square of the following diagram is not commutative:

$$\begin{array}{ccccc} \mathrm{Enc}_1(\mathcal{M}_1) & \hookrightarrow & \mathcal{C}_1 & \xrightarrow{\quad f \quad} & \mathcal{C}_2 \\ & & \downarrow{\scriptstyle \mathrm{Dec}_1} & & \downarrow{\scriptstyle \mathrm{Dec}_2} \\ & & \mathcal{M}_1 & \xrightarrow{\quad \iota \quad} & \mathcal{M}_2 \end{array}$$

where f is a bridge between encryption schemes. Indeed, the definition of a bridge is imposing commutativity only for the restriction of f to $\mathrm{Enc}_1(\mathcal{M}_1) \subseteq \mathcal{C}_1$, i.e. to the subset of the ciphertext space which consists of *fresh encryptions*. This observation leads to the following definition.

Definition 6. *Let $\mathcal{E}_i = (\mathcal{M}_i, \mathcal{C}_i, \mathrm{KeyGen}_i, \mathrm{Enc}_i, \mathrm{Dec}_i)$, $i \in \{1, 2\}$ be two encryption schemes. A bridge $\mathbf{B}_{\iota,f}$ from $\mathcal{E}_1$ to $\mathcal{E}_2$ is called* ***complete*** *if the PPT algorithm f, which takes as input the bridge key bk and* any *ciphertext $c_1 \in \mathcal{C}_1$ satisfies the equality*

$$\mathrm{Dec}_2(sk_2, f(bk, c_1)) = \iota(\mathrm{Dec}_1(sk_1, c_1)),$$

for any the triple (sk_1, sk_2, bk) outputted by the key generation algorithm of the bridge.

Let us notice the following easy fact:

Remark 3. Suppose that $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ is an encryption scheme. If for every pair $(sk, pk) \leftarrow \mathrm{KeyGen}(1^\lambda)$ and every $c \in \mathcal{C}$ there exists a $m \in \mathcal{M}$ such that $c \in \mathrm{Enc}(pk, m)$, then any bridge from $\mathcal{E}$ to any other scheme, is complete.

As a consequence, the bridge from the Goldwaser-Micali (GM) encryption scheme to the Sander-Young-Yung (SYY) encryption scheme described in [3] is complete. Indeed, the GM encryption scheme does enjoy the property described in the above remark: for any two distinct primes p, q, every element from the ciphertext space $J_1(pq)$ can be obtained as an encryption $\mathrm{Enc}_{GM}(pq, m)$ of some plaintext $m \in \mathbb{Z}_2$.

An example of a different flavor arises from the modulus switching procedure, which is frequently used in homomorphic encryption schemes for different purposes (such as reducing the noise of a ciphertext).

Example 2. Let q, Q be two integers such that q divides Q. For simplicity, assume that $q, Q \equiv 2 \pmod 4$. We let $\mathrm{LWE}^{2/q}$ and $\mathrm{LWE}^{2/Q}$ be the LWE encryption schemes with plaintext spaces $\mathcal{M} = \mathbb{Z}_2$ and ciphertext modulus q and Q, respectively (see [20]).

Recall that a ciphertext encrypting the message m in $\mathrm{LWE}^{2/q}$ is of the form (a, b), where $a \leftarrow \mathbb{Z}_q^n$ is sampled uniformly and $b = \langle a, s\rangle + m \cdot \frac{q}{2} + e$, where e is drawn from the noise distribution.

The decryption can be regarded as a map from $\mathbb{Z}_q^n \times \mathbb{Z}_q$ to $\mathbb{Z}_2$, given by

$$\mathrm{Dec}_q\,(a, b) = \begin{cases} 0, \text{ if } b - \langle a, s\rangle \in (-q/4, q/4) \\ 1, \text{ otherwise.} \end{cases}$$

We define a bridge f from $\mathrm{LWE}^{2/q}$ to $\mathrm{LWE}^{2/Q}$, as follows. In the second stage, the bridge key generation algorithm takes as input $s \in \mathbb{Z}_q^n$, the secret key of $\mathrm{LWE}^{2/q}$, and generates the same key for $\mathrm{LWE}^{2/Q}$, viewed in $\mathbb{Z}_Q^n$. Finally, this algorithm outputs an empty bridge key.

The algorithm f will take as input a ciphertext $(a, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ and computes $\left(\frac{Q}{q} \cdot a, \frac{Q}{q} \cdot b\right) \in \mathbb{Z}_Q^n \times \mathbb{Z}_Q$. It is not hard to see that this bridge is complete.

This resembles the modulus-switching procedures used initially to simplify the decryption circuit in [7] and later to reduce the noise accumulated after homomorphic multiplication in [6]. We note that in modulus-switching procedures the ciphertexts are converted from a larger modulus Q, to a smaller one q, whereas in the example described above the procedures go from a smaller modulus to a larger one.

However, let us remark that, one can always modify the decryption algorithm in $\mathrm{LWE}^{2/q}$ to obtain a complete bridge to $\mathrm{LWE}^{2/Q}$ even when the modulus Q is smaller than q.

It will become apparent in the following that the completeness property of a bridge plays an important role in being able to move an encryption through a chain of bridges without performing any decryption. This triggers one of the main notions presented in this paper, namely the composability of bridges which shall be discussed in details in what follows.

Given two bridges $f : \mathcal{E}_1 \to \mathcal{E}_2$, $g : \mathcal{E}_2 \to \mathcal{E}_3$, between encryption schemes $\mathcal{E}_1$ and $\mathcal{E}_2$ respectively $\mathcal{E}_2$ and $\mathcal{E}_3$, it is desirable to be able to use them, in order to convert a ciphertext from $\mathcal{E}_1$ to $\mathcal{E}_3$ while preserving the underlying plaintext. If possible, such a procedure should resemble the composition of two functions. In particular, it is obvious that to achieve such a conversion, the Key Generation algorithms of f and g should not run independently, as we now explain in the following construction/definition:

Definition 7 (Composition of bridges). *Let $f : \mathcal{E}_1 \to \mathcal{E}_2$ and $g : \mathcal{E}_2 \to \mathcal{E}_3$ be bridges between the encryption schemes $\mathcal{E}_1, \mathcal{E}_2$, and $\mathcal{E}_2, \mathcal{E}_3$, respectively. The composition of $g \circ f$ consists of the following procedures:*

1. *The function $\iota_{g\circ f} := \iota_g \circ \iota_f : \mathcal{P}_1 \to \mathcal{P}_3$, which is computable by a deterministic polynomial time algorithm.*

2. *A PPT bridge key generation algorithm, which runs as follows. First, it takes the security parameter λ and runs the Key Generation algorithm of f to obtain $(sk_1, pk_1, sk_2, pk_2, bk_f)$. After that, it only uses the second and third stages of the Key Generation of g to obtain (sk_3, pk_3, bk_g). Finally, it outputs the bridge key $bk_{g\circ f} = (bk_f, pk_2, bk_g)$.*
3. *A PPT algorithm $g \circ f$ which takes as input a ciphertext $c_1 \in \mathcal{C}_1$ and outputs $g(bk_g, f(bk_f, c_1))$.*

A first observation is that, unfortunately, the composition of two bridges is not necessarily a bridge. Indeed, due to the fact that for $m \in \mathcal{P}_1$, the ciphertext $f(bk_1, \mathrm{Enc}_1(pk_1, m))$ is not necessarily a fresh encryption of $\iota_f(m)$, the correctness properties of f and g do not imply that

$$\mathrm{Dec}_3(sk_3, (g \circ f)(bk_{g\circ f}, \mathrm{Enc}_1(pk_1, m)) = \iota_{g\circ f}(m).$$

This feature will also be present in the case of bridges constructed from circuits in section 7 and it was pointed out before in a presentation by Micciancio [27].

On the other hand, if the second bridge of a pair of bridges is complete, then the composition is also a bridge as the following proposition states.

Proposition 1. *Let $f : \mathcal{E}_1 \to \mathcal{E}_2$ and $g : \mathcal{E}_2 \to \mathcal{E}_3$ be bridges between the encryption schemes $\mathcal{E}_1, \mathcal{E}_2$ and $\mathcal{E}_3$, such that g is complete. Then, the composition $g \circ f : \mathcal{E}_1 \to \mathcal{E}_3$ is a bridge.*

Proof. Since g is complete, the correctness property for g holds for any ciphertext. In particular, it holds for ciphertexts of the form $f(bk_1, \mathrm{Enc}_1(pk_1, m))$, so that we have:

$$\begin{aligned}\mathrm{Dec}_3(sk_3, (g \circ f)(bk_{g\circ f}, \mathrm{Enc}_1(pk_1, m))) &= \iota_g(\mathrm{Dec}_2(sk_2, f(bk_f, \mathrm{Enc}_1(pk_1, m)))) \\ &= \iota_g(\iota_f(m)) = \iota_{g\circ f}(m),\end{aligned}$$

where the first equality follows from the completeness of g and the second equality from the correctness property of f.

To end the discussion of this section we introduce the following definition:

Definition 8. *A pair of bridges (f, g) is called* composable *if $g \circ f$ is defined and is also a bridge.*

We have the following consequence of the last proposition:

Corollary 1. *If $f : \mathcal{E}_1 \to \mathcal{E}_2$ and $g : \mathcal{E}_2 \to \mathcal{E}_3$ are two complete bridges then they are composable and their composition is complete.*

Proof. The proof follows immediately using the same argument as in the proof of the last Proposition.

Remark 4. Since complete bridges behave well with respect to composition, they form the class of morphisms of a category.

5 On the security of composition of bridges

The aim of this section is to investigate the security of the composition of two bridges. We shall introduce first the security notions related to the security of a bridge without giving all the details (for a full account see [3]). Then we prove our main theorems stating that the composition of secure bridges is secure under a certain technical condition. In the next section we shall prove that this condition is satisfied by an important class of bridges.

Given a public-key encryption scheme $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ and an adversary $\mathcal{A}$ consider the following the IND-CPA experiment $\mathrm{Expr}^{\mathrm{IND-CPA}}[\mathcal{A}]$:

1. Run $\mathrm{KeyGen}(1^\lambda)$ to obtain the pair of keys (sk, pk).
2. The key pk is given to the adversary $\mathcal{A}$. It outputs a pair of messages m_0, m_1 of its choice.
3. The challenger chooses a uniform bit $b \in \{0, 1\}$, and then a ciphertext $c \leftarrow \mathrm{Enc}(pk, m_b)$ is computed and given to $\mathcal{A}$.
4. The adversary $\mathcal{A}$ outputs a bit b'.
5. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise.

Definition 9 (IND-CPA Security). *The advantage of adversary $\mathcal{A}$ against the IND-CPA security of the scheme is $\mathcal{E}$ is defined by*

$$\mathrm{Adv}^{\mathrm{IND-CPA}}[\mathcal{A}](\lambda) := |\Pr\{\mathrm{Expr}^{\mathrm{IND-CPA}}[\mathcal{A}] = 1\} - \Pr\{\mathrm{Expr}^{\mathrm{IND-CPA}}[\mathcal{A}] = 0\}|,$$

where the probability is over the randomness of $\mathcal{A}$ and of the experiment. A public key encryption scheme $\mathcal{E}$ has indistinguishable encryptions under chosen-plaintext attack (or is IND-CPA-secure) if for any probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negligible function negl *such that*

$$\mathrm{Adv}^{\mathrm{IND-CPA}}[\mathcal{A}](\lambda) = \mathrm{negl}(\lambda).$$

Remark 5. As it is well known (see for instance Proposition 5.9 in [4]), an encryption scheme is IND-CPA-secure if and only if for any PPT-adversary $\mathcal{A}$ there exists a negligible function negl such that

$$\Pr[\mathrm{Expr}^{\mathrm{IND-CPA}}[\mathcal{A}] = 1](\lambda) \leq \frac{1}{2} + \mathrm{negl}(\lambda).$$

In [3], the authors associated to any bridge $f : \mathcal{E}_1 \to \mathcal{E}_2$ an encryption scheme $\mathcal{G}_f$ (called the graph of the bridge) and defined the security of the bridge as being the security of the associated scheme $\mathcal{G}_f$. On the other hand, they proved that the security of $\mathcal{G}_f$ is equivalent to the security of $\mathcal{E}_1[pk_2, bk_f]$ which is the encryption scheme $\mathcal{E}_1$ endowed with additional public information given by the public key of $\mathcal{E}_2$ and the bridge key of f (for further details, see [3, Theorem 1]). Hereafter, we propose this equivalent notion as the security of a bridge because in practice it is much easier to work with it.

Since we will make use of the explicit construction of $\mathcal{G}_f$ in our arguments, we shall briefly recall its structure (for more details see the Section 3 of [3]):

- The plaintext space of $\mathcal{G}_f$ is the same as the plaintext space of $\mathcal{E}_1$, that is $\mathcal{M}_1$. The ciphertext space is $\mathcal{C}_1 \times \mathcal{C}_2$, where $\mathcal{C}_i$ is the ciphertext space of $\mathcal{E}_i$, $\forall i \in \{1, 2\}$.
- The secret key of $\mathcal{G}_f$ is the pair: $sk_{\mathcal{G}_f} := (sk_1, sk_2)$.
- The public key is the triple: $pk_{\mathcal{G}_f} := (pk_1, pk_2, bk_f)$.
- The encryption algorithm is given by

$$\mathrm{Enc}_{\mathcal{G}_f}(pk_{\mathcal{G}_f}, m) := (\mathrm{Enc}_1(pk_1, m), f(bk_f, \mathrm{Enc}_1(pk_1, m))),$$

  for all $m \in \mathcal{M}_1$.
- The decryption algorithm is $\mathrm{Dec}_{\mathcal{G}_f}(sk_{\mathcal{G}_f}, (a, b)) := \mathrm{Dec}_1(sk_1, a)$.

In what follows we are interested in finding conditions that ensure the security of a bridge obtained as a composition of two composable bridges. The following easy result, can be seen as a necessary condition for the security of such a bridge.

Proposition 2. *Suppose $f : \mathcal{E}_1 \to \mathcal{E}_2$ and $g : \mathcal{E}_2 \to \mathcal{E}_3$ are composable bridges, such that $g \circ f$ is a secure bridge. Then f is a secure bridge.*

Proof. Since the bridge key of $g \circ f$ is given by $bk_{g \circ f} = (bk_f, pk_2, bk_g)$, the security of f follows from the above considerations.

On the other hand, if the composition $g \circ f$ is a secure bridge, it does not follow that g is secure. Let us illustrate this with the following example.

Example 3. Assume that $f : \mathcal{E}_1 \to \mathcal{E}_2$ and $g : \mathcal{E}_2 \to \mathcal{E}_3$ are composable secure bridges such that $g \circ f$ is secure. By [3, Proposition 1], the encryption schemes $\mathcal{E}_1$ and $\mathcal{E}_2$ are IND-CPA secure. For simplicity, assume that the common plaintext is $\mathcal{M} = \{0, 1\}$. We now construct the encryption scheme $\mathcal{E}_2'$, as follows: this scheme is almost identical to $\mathcal{E}_2$, except that the encryption reveals the message. More precisely, $\mathrm{Enc}_2'(pk_2, m) = (\mathrm{Enc}_2(pk_2, m), m)$ is a concatenation of the encryption of m in the scheme $\mathcal{E}_2$ with the plaintext m itself. This new encryption scheme $\mathcal{E}_2'$ is obviously not secure.

On the other hand, we modify f and g to new bridges f' and g' in the following way. For any ciphertext $c \in \mathcal{C}_1$, we let $f'(c_1) = (f(c_1), b)$, where $b \leftarrow \{0, 1\}$ is chosen uniformly at random. The bridge g' will perform as follows. For any ciphertext $c_2' = (c_2, b) \in \mathcal{C}_2'$, we let $g'(c_2') = g(c_2) \in \mathcal{C}_3$. It can be easily verified that $g' \circ f'$ is a secure bridge from $\mathcal{E}_1 \to \mathcal{E}_3$. However, the bridge g' is not secure because the modified encryption scheme $\mathcal{E}_2'$ is not secure.

Next, we give an example of two (complete) secure bridges f and g, which are composable, for which $g \circ f$ is an insecure bridge.

Example 4. Consider $\mathcal{E}$ an encryption scheme (not homomorphic or with any other special property). We shall assume that knowing half of the secret key does not harm the security. Denote by $\ell(\lambda)$ the bit length of its secret key. We define $\mathcal{E}_1$ to be $\mathcal{E}$, while $\mathcal{E}_2$ is $\mathcal{E}$ with a modified cyphertext space, consisting of concatenations of cyphertexts of $\mathcal{E}$ with strings of length $\ell(\lambda)/2$. The encryption algorithm in $\mathcal{E}_2$ outputs a concatenation of an encryption of $\mathcal{E}$ with

a random sequence of length $\ell(\lambda)/2$. The decryption algorithm is just the decryption algorithm of $\mathcal{E}$ applied to the first part of the ciphertext, i.e. the bit string corresponding to a ciphertext in the scheme $\mathcal{E}$. Also, consider $\mathcal{E}_3$ to be the scheme obtained by applying on $\mathcal{E}_2$ the same procedure used in the construction of $\mathcal{E}_2$ from $\mathcal{E}$.

The bridge key of $f : \mathcal{E}_1 \to \mathcal{E}_2$ consists of the first half of the bit representation of the secret key of $\mathcal{E}$ and f is defined by the concatenation of the identity map with the bridge key. The bridge $g : \mathcal{E}_2 \to \mathcal{E}_3$ has a similar construction, only that the bridge key of g consists of the second half of the secret key of $\mathcal{E}$. Now, by our assumptions, the schemes $\mathcal{E}[bk_f]$ and $\mathcal{E}[bk_g]$ are secure. Hence, the bridges f and g are secure. Moreover, f and g are clearly complete, thus composable.

However, their composition reveals the entire secret key because the bridge key of the composition contains both halves of the secret key of $\mathcal{E}$. Schemes $\mathcal{E}$ satisfying the above conditions are plenty in the literature. For example any LWE scheme is such.

From these examples we learn that an additional condition on a pair of composable bridges is required in order to get a secure composition.

This motivates our main result, that is Theorem 2. This result is heavily influenced by the main result of [3], which we recall first together with a more conceptual proof.

Suppose $\mathbf{B}_{\iota,f}$ is a bridge from $\mathcal{E}_1$ to $\mathcal{E}_2$. Recall that the *bridge key generation algorithm* produces the following ensembles of $\{\mathcal{SK}_{1,\lambda}\}_\lambda$ distributions: $\{\mathcal{PK}_{1,\lambda}\}_\lambda$, $\{\mathcal{PK}_{2,\lambda}\}_\lambda$ and $\{\mathcal{BK}_\lambda\}_\lambda$. Let $\mathcal{F}$ be the ensemble of finite distributions of triples (pk_1, pk_2, bk). Recall that $\pi_1 : \mathcal{F} \to \mathcal{PK}_1$ is a morphism of finite distributions, so $\mathcal{F}$ is an ensemble of $\mathcal{PK}_1$-distributions. In this theorem, we will make use for the first time of the Definitions 1 and 2.

Theorem 1. *Let $\mathbf{B}_{\iota,f}$ be a bridge between $\mathcal{E}_1$ and $\mathcal{E}_2$ and assume that the scheme $\mathcal{E}_1$ is IND-CPA secure. If there exists a polynomial time constructible on fibers ensemble of $\mathcal{PK}_1$-distributions $\widetilde{\mathcal{F}}$ which is computational indistinguishable from $\mathcal{F}$, then the bridge $\mathbf{B}_{\iota,f}$ is IND-CPA secure.*

Proof. To show that the bridge $\mathbf{B}_{\iota,f}$ is IND-CPA secure it is enough to show that for any attacker $\mathcal{A}$ on $\mathcal{E}_1[\mathcal{PK}_{\mathcal{G}_f}]$ the probability of answering correctly is bounded above by $\frac{1}{2} + \mathrm{negl}(\lambda)$ (see Remark 5). This probability is given by

$$\Pr[\mathrm{Expr}[\mathcal{A}] = 1] = \frac{1}{2}\Pr[\mathcal{A}(\mathcal{F}, \mathrm{Enc}_1(pk_1, 0)) = 0] + \frac{1}{2}\Pr[\mathcal{A}(\mathcal{F}, \mathrm{Enc}_1(pk_1, 1)) = 1].$$

If $\mathcal{A}$ is any attacker on $\mathcal{E}_1[\mathcal{PK}_{\mathcal{G}_f}]$, then we construct an attacker $\mathcal{A}_1$ on $\mathcal{E}_1$ as follows: $\mathcal{A}_1$ receives the pair $(pk_1, c \leftarrow \mathrm{Enc}_1(pk_1, b))$ from the challenger and uses the sampling algorithm of $\widetilde{\mathcal{F}}$ to produce a triple (pk_1, α, β). The attacker gives (pk_1, α, β, c) to $\mathcal{A}$ and then outputs the bit received from it. Since $\mathcal{E}_1$ is IND-CPA secure we have

$$\Pr[\mathrm{Expr}[\mathcal{A}_1] = 1] \leq \frac{1}{2} + \mathrm{negl}_1(\lambda),$$

for some negligible function $\mathrm{negl}_1(\lambda)$. We get that

$$\begin{aligned}\Pr[\mathrm{Expr}[\mathcal{A}_1]=1] &= \frac{1}{2}\Pr[\mathcal{A}(\widetilde{\mathcal{F}},\mathrm{Enc}_1(pk_1,0))=0]+\frac{1}{2}\Pr[\mathcal{A}(\widetilde{\mathcal{F}},\mathrm{Enc}_1(pk_1,1))=1]\\ &\leq \frac{1}{2}+\mathrm{negl}_1(\lambda).\end{aligned} \tag{1}$$

We construct now an IND-CPA distinguisher $\mathcal{D}_0$ between $\mathcal{F}$ and $\widetilde{\mathcal{F}}$ as follows. The distinguisher receives a triple (pk_1, x, y) from the challenger and uses pk_1 to compute $c \leftarrow \mathrm{Enc}_1(pk_1, 0)$, gives (pk_1, x, y, c) to $\mathcal{A}$ and outputs the bit received from $\mathcal{A}$. We understand that $\mathrm{Expr}[\mathcal{D}_0]$ identifies $\mathcal{F}$ if it outputs 0 and $\widetilde{\mathcal{F}}$, if it outputs 1. Then we have:

$$\begin{aligned}\Pr[\mathrm{Expr}[\mathcal{D}_0]=1] &= \frac{1}{2}\Pr[\mathcal{A}(\mathcal{F},\mathrm{Enc}_1(pk_1,0))=0]+\frac{1}{2}\Pr[\mathcal{A}(\widetilde{\mathcal{F}},\mathrm{Enc}_1(pk_1,0))=1]\\ &\leq \frac{1}{2}+\mathrm{negl}_2(\lambda).\end{aligned} \tag{2}$$

Similarly, one constructs $\mathcal{D}_1$, a distinguisher between $\widetilde{\mathcal{F}}$ and $\mathcal{F}$, similarly as above, but now $c \leftarrow \mathrm{Enc}_1(pk_1, 1)$. This time, $\mathrm{Expr}[\mathcal{D}_1]$ outputs 0 if the distinguisher identifies $\widetilde{\mathcal{F}}$ and outputs 1 if the distinguisher identifies $\mathcal{F}$. Thus, we get:

$$\begin{aligned}\Pr[\mathrm{Expr}[\mathcal{D}_1]=1] &= \frac{1}{2}\Pr[\mathcal{A}(\mathcal{F},\mathrm{Enc}_1(pk_1,1))=1]+\frac{1}{2}\Pr[\mathcal{A}(\widetilde{\mathcal{F}},\mathrm{Enc}_1(pk_1,1))=0]\\ &\leq \frac{1}{2}+\mathrm{negl}_3(\lambda).\end{aligned} \tag{3}$$

Adding the inequalities (1), (2), (3) and using the equalities:

$$\Pr[\mathcal{A}(\widetilde{\mathcal{F}},\mathrm{Enc}_1(pk_1,0))=0]+\Pr[\mathcal{A}(\widetilde{\mathcal{F}},\mathrm{Enc}_1(pk_1,0))=1]=1$$

$$\Pr[\mathcal{A}(\widetilde{\mathcal{F}},\mathrm{Enc}_1(pk_1,1))=0]+\Pr[\mathcal{A}(\widetilde{\mathcal{F}},\mathrm{Enc}_1(pk_1,1))=1]=1$$

we obtain

$$\frac{1}{2}\Pr[\mathcal{A}(\mathcal{F},\mathrm{Enc}_1(pk_1,0))=0]+\frac{1}{2}\Pr[\mathcal{A}(\mathcal{F},\mathrm{Enc}_1(pk_1,1))=1]\leq\frac{1}{2}+\mathrm{negl}(\lambda),$$

which is exactly what we wanted to prove.

Now, we are able to state and prove our main result.

Theorem 2. *Suppose $f : \mathcal{E}_1 \to \mathcal{E}_2$, $g : \mathcal{E}_2 \to \mathcal{E}_3$ are composable bridges such that f is IND-CPA secure and there exists a polynomial time constructible on fibers ensemble of $\mathcal{PK}_f-$distributions which is computational indistinguishable from $\mathcal{PK}_{g\circ f}$, then $g \circ f$ is IND-CPA secure.*

Proof. Notice that the composable pair of bridges (f, g) gives rise to a bridge $\widehat{g} : \mathcal{G}_f \to \mathcal{E}_3$, by the formula:

$$\widehat{g}(bk_{\hat{g}}, (a, b)) := g(bk_g, b),$$

where $bk_{\hat{g}} = bk_g$. Since f is secure, it follows that the scheme $\mathcal{G}_f$ is secure. By our assumptions, an immediate application of Theorem 1 shows that $\widehat{g}$ is IND-CPA secure, which means that the scheme $\mathcal{G}_{\widehat{g}}$ is IND-CPA secure. Notice that an encryption of a message m in $\mathcal{G}_{\widehat{g}}$ is in fact a triple of the form $(a, f(bk_f, b), g(bk_g, f(bk_f, c)))$, where a, b, c are encryptions of m in $\mathcal{E}_1$, so that any adversary $\mathcal{A}$ on $\mathcal{G}_{g\circ f}$ gives rise to an adversary $\mathcal{A}'$ on $\mathcal{G}_{\widehat{g}}$. Indeed, notice first that these encryption schemes have the same public key. On the other hand if $(a, f(bk_f, b), g(bk_g, f(bk_f, c)))$ is the triple received by $\mathcal{A}'$ from the challenger (together with the public key), then $\mathcal{A}'$ gives the public key and the pair $(a, g(bk_g, f(bk_f, c)))$ to $\mathcal{A}$ and outputs the bit received from it. It is easy to see that, since

$$\Pr[\mathrm{Expr}^{\mathrm{IND-CPA}}[\mathcal{A}'](\lambda) = 1] = \Pr[\mathrm{Expr}^{\mathrm{IND-CPA}}[\mathcal{A}](\lambda) = 1],$$

if the attacker $\mathcal{A}$ breaks the IND-CPA security of $\mathcal{G}_{g\circ f}$, then $\mathcal{A}'$ also breaks the security of $\mathcal{G}_{\widehat{g}}$, and this is a contradiction.

6 Gentry type bridges

We recall the construction of Gentry type bridges from [3]. Briefly, the *Recrypt* algorithm, used in the bootsrapping procedure that transforms a somewhat homomorphic encryption scheme into a fully homomorphic encryption scheme (see [22]), can be adapted to our situation in order to give a general recipe for the construction of a bridge.

Let us consider an encryption scheme

$$\mathcal{E} = (\mathrm{KeyGen}_{\mathcal{E}}, \mathrm{Enc}_{\mathcal{E}}, \mathrm{Dec}_{\mathcal{E}})$$

and a homomorphic encryption scheme

$$\mathcal{H} = (\mathrm{KeyGen}_{\mathcal{H}}, \mathrm{Enc}_{\mathcal{H}}, \mathrm{Dec}_{\mathcal{H}}, \mathrm{Eval}_{\mathcal{H}}).$$

We shall also denote by $\mathcal{M}_{\mathcal{E}}, \mathcal{C}_{\mathcal{E}}$ and $\mathcal{M}_{\mathcal{H}}, \mathcal{C}_{\mathcal{H}}$, the plaintext and ciphertext spaces of $\mathcal{E}$ and $\mathcal{H}$, respectively.

Fix once and for all, a function $\iota : \mathcal{M}_{\mathcal{E}} \to \mathcal{M}_{\mathcal{H}}$ that is computable by a deterministic polynomial time algorithm.

At a high level, the bridge key bk_f of a Gentry-type bridge $f : \mathcal{E} \to \mathcal{H}$ consists of the bit representation of the secret key of $\mathcal{E}$ encrypted under the public key of

$\mathcal{H}$. Moreover, the bridge algorithm is the homomorphic evaluation of the circuit $\iota \circ \mathrm{Dec}_{\mathcal{E}} : \mathcal{C}_{\mathcal{E}} \to \mathcal{M}_{\mathcal{H}}$.

We now describe with details the algorithms of the bridge. Let us start with the key generation algorithm.

• In the first stage, the key generation algorithm of the bridge runs $\mathrm{KeyGen}_{\mathcal{E}}(1^{\lambda})$ to obtain a pair of keys $(sk_{\mathcal{E}}, pk_{\mathcal{E}})$. The second stage of the algorithm runs independently of the first one, and it just makes use of $\mathrm{KeyGen}_{\mathcal{H}}(1^{\lambda})$ to obtain $(sk_{\mathcal{H}}, pk_{\mathcal{H}})$.

The final stage of the algorithm takes as input $(sk_{\mathcal{E}}, pk_{\mathcal{E}}, sk_{\mathcal{H}}, pk_{\mathcal{H}})$ constructed as above, and creates bk_f as the vector of encryptions of the bit representation of $sk_{\mathcal{E}}$ under $pk_{\mathcal{H}}$ (the details of this are below).

• The PPT algorithm f mentioned in the third part of Definition 4 is the homomorphic evaluation of the algorithm $\iota \circ \mathrm{Dec}_{\mathcal{E}}$. To rigorously perform it, we need to realise $\iota \circ \mathrm{Dec}_{\mathcal{E}}$ as a map $\mathcal{M}_{\mathcal{H}}^{\ell} \to \mathcal{M}_{\mathcal{H}}$, and for this we use the ring structure on $\mathcal{M}_{\mathcal{H}}$ (we shall assume that such a ring structure exists; one can avoid this assumption with little work, but since all the known FHE schemes have this property we chose to work with it). Suppose that the ciphertext space $\mathscr{C}_{\mathcal{E}}$ has a representation as a subset of $\{0,1\}^n$ and that the set of secret keys is a subset of $\{0,1\}^e$, so that $\iota \circ \mathrm{Dec}_{\mathcal{E}} : \{0,1\}^e \times \{0,1\}^n \to \mathcal{M}_{\mathcal{H}}$. Now, we construct the map $\widetilde{\iota \circ \mathrm{Dec}_{\mathcal{E}}} : \mathcal{M}_{\mathcal{H}}^e \times \mathcal{M}_{\mathcal{H}}^n \to \mathcal{M}_{\mathcal{H}}$ as follows. Viewing $\mathcal{M}_{\mathcal{H}}$ as a subset of $\{0,1\}^m$, we have that $\iota \circ \mathrm{Dec}_{\mathcal{E}} : \{0,1\}^e \times \{0,1\}^n \to \mathcal{M}_{\mathcal{H}}$ is a vector $(g_1, ..., g_m)$ of boolean circuits expressed using XOR and AND gates. Let $\tilde{g}_i : \mathcal{M}_{\mathcal{H}}^e \times \mathcal{M}_{\mathcal{H}}^n \to \mathcal{M}_{\mathcal{H}}$ be the circuit obtained by replacing each $\mathrm{XOR}(x,y)$ gate by $x \oplus y := 2(x+y) - (x+y)^2$ and each $\mathrm{AND}(x,y)$ gate by $x \otimes y := x \cdot y$, where $+$ and $\cdot$ are the addition and multiplication in $\mathcal{M}_{\mathcal{H}}$. Notice that the subset of $\mathcal{M}_{\mathcal{H}}$ consisting of its zero element $0_{\mathcal{H}}$ and its unit $1_{\mathcal{H}}$ together with $\oplus$ and $\otimes$ is a realisation of the field with two elements inside $\mathcal{M}_{\mathcal{H}}$. In other words, if $c = (c[1], ..., c[n]) \in \mathscr{C}_{\mathcal{E}}$ and $sk_{\mathcal{E}} = (sk[1], ..., sk[e])$ is the secret key, then $\tilde{g}_i(sk[1]_{\mathcal{H}}, ..., sk[e]_{\mathcal{H}}, c[1]_{\mathcal{H}}, ..., c[n]_{\mathcal{H}}) = m_{\mathcal{H}}$ if $g_i(sk[1], ..., sk[e], c[1], ..., c[n]) = m$ for all i, where $m \in \{0,1\}$. For an element $x \in \mathcal{M}_{\mathcal{H}}$, we let $[x = 1_{\mathcal{H}}]$ be the equality test, which returns 1 if $x = 1_{\mathcal{H}}$ and 0 otherwise. Finally, $\widetilde{\iota \circ \mathrm{Dec}_{\mathcal{E}}} : \mathcal{M}_{\mathcal{H}}^e \times \mathcal{M}_{\mathcal{H}}^n \to \{0,1\}^m$ is defined by:

$$([\tilde{g}_i(y_1, ..., y_e, x_1, ..., x_n) = 1_{\mathcal{H}}])_{i=\overline{1,m}}.$$

One can verify immediately that

$$\widetilde{\iota \circ \mathrm{Dec}_{\mathcal{E}}}(sk[1]_{\mathcal{H}}, ..., sk[e]_{\mathcal{H}}, c[1]_{\mathcal{H}}, ..., c[n]_{\mathcal{H}}) = \iota \circ \mathrm{Dec}_{\mathcal{E}}(sk_{\mathcal{E}}, c).$$

Now we are ready to define the bridge algorithm f. Given a ciphertext $c \in \mathscr{C}_{\mathcal{E}}$, the algorithm f first encrypts the bits of c (viewed as elements of $\mathcal{M}_{\mathcal{H}}$) under $pk_{\mathcal{H}}$ and retains these encryptions in a vector $\tilde{c}$. The bridge key bk_f is obtained by encrypting the bits $sk[i]_{\mathcal{E}}$ under $pk_{\mathcal{H}}$, for $i \in \overline{1,e}$. Then, the algorithm f outputs $\mathrm{Eval}_{\mathcal{H}}(evk_{\mathcal{H}}, \widetilde{\iota \circ \mathrm{Dec}_{\mathcal{E}}}, (bk_f, \tilde{c}))$.

Remark 6. Let us notice that in the above construction, one does not necessarily need to encrypt the bit representation of the ciphertext c under $pk_{\mathcal{H}}$. The whole

construction works if one homomorphically evaluates the circuits $\widetilde{\iota \circ \mathrm{Dec}_{\mathcal{E}}}(\cdot, c) : \mathcal{M}_{\mathcal{H}}^{e} \to \mathcal{M}_{\mathcal{H}}$, for each fixed ciphertext c. While this variant is often more efficient, one needs to compute the circuit $\widetilde{\iota \circ \mathrm{Dec}_{\mathcal{E}}}(\cdot, c)$ every time the bridge is applied. Also, most of the time, there exist "trivial" encryptions of $0_{\mathcal{H}}$ and $1_{\mathcal{H}}$, so that the two bridges become identical.

Theorem 3. *Any Gentry type bridge is complete.*

Proof. With the above notations, if c is *any* ciphertext in $\mathcal{C}_{\mathcal{E}}$, then $\tilde{c}$ consists of an n-dimensional vector of "fresh" encryptions of the scheme $\mathcal{H}$. Since bk_f is an e-dimensional vector consisting of fresh encryptions, we have:

$$\begin{aligned}\mathrm{Dec}_{\mathcal{H}}(sk_{\mathcal{H}}, f(bk_f, c)) &= \mathrm{Dec}_{\mathcal{H}}\left(sk_{\mathcal{H}}, \mathrm{Eval}_{\mathcal{H}}(evk_{\mathcal{H}}, \widetilde{\iota \circ \mathrm{Dec}}_{\mathcal{E}}, (bk_f, \tilde{c}))\right)\\ &= (\iota \circ \mathrm{Dec}_{\mathcal{E}})\left(\mathrm{Dec}_{\mathcal{H}}(sk_{\mathcal{H}}, bk_f), \mathrm{Dec}_{\mathcal{H}}(sk_{\mathcal{H}}, \tilde{c})\right)\\ &= \iota\left(\mathrm{Dec}_{\mathcal{E}}(sk_{\mathcal{E}}, c)\right)\end{aligned}$$

which shows that third condition in the definition of a bridge is satisfied for any ciphertext $c \in \mathscr{C}_{\mathcal{E}}$, i.e. f is complete.

An immediate consequence of this theorem and Proposition 1 is the following:

Corollary 2. *If $f : \mathcal{E}_1 \to \mathcal{E}_2$ is a bridge and $g : \mathcal{E}_2 \to \mathcal{H}$ is a Gentry type bridge, then the two bridges are composable.*

Now, we can state and prove the main result of this section.

Theorem 4. *If $f : \mathcal{E}_1 \to \mathcal{E}_2$ is a secure bridge, $g : \mathcal{E}_2 \to \mathcal{H}$ is a Gentry type secure bridge, and $\mathcal{H}$ is a secure FHE scheme, then $g \circ f$ is a secure bridge.*

Proof. The security of the bridge will follow from Theorem 2, after showing that the ensemble of distributions $\mathcal{PK}_{g\circ f}$ satisfies the required indistinguishably condition with respect to a certain polynomial-time constructible on fibers $\mathcal{PK}_f$-distribution. Let us recall that $\mathcal{PK}_f$ consists of the tuple (pk_1, pk_2, bk_f) and that $\mathcal{PK}_{g\circ f}$ consists of $(pk_1, pk_2, bk_f, pk_{\mathcal{H}}, bk_g)$. As g is of Gentry-type, bk_g consists of a vector encrypting the bit representation of sk_2 under $pk_{\mathcal{H}}$. Let $\tilde{\mathcal{F}}$ be the ensemble of distributions $(pk_1, pk_2, bk_f, pk_H, \widetilde{bk})$, obtained in the following way. Firstly, one samples (pk_1, pk_2, bk_f) from the distribution $\mathcal{PK}_f$. Secondly, one uses $\mathrm{KeyGen}_{\mathcal{H}}$ to sample $pk_{\mathcal{H}}$ and then we let $\widetilde{bk} = (\widetilde{bk}[1], ..., \widetilde{bk}[e])$ with $\widetilde{bk}[i] \leftarrow \mathrm{Enc}(pk_{\mathscr{H}}, 0_{\mathscr{H}})$ for all $i \in \overline{1, e}$, where e is the bit-length of sk_2. Note that e can be considered public knowledge, as it only depends on the parameters of encryption in the scheme $\mathcal{E}_2$. We also note that since g is a Gentry type bridge, the public key $pk_{\mathcal{H}}$ and any sample from the distribution $\mathcal{PK}_f$ are chosen independently from each other. Note that $\tilde{\mathcal{F}}$ is a polynomial-time constructible on fibers $\mathcal{PK}_f$-distribution. If the scheme $\mathcal{H}$ is IND-CPA secure, then one can prove by a hybrid argument, identical to the one in the proof of Proposition 2 of [3], that the $\mathcal{PK}_f$-distributions $\mathcal{PK}_{g\circ f}$ and $\tilde{\mathcal{F}}$ are computationally indistinguishable.

Remark 7. Notice that the Gentry type bridge g in the above theorem is already secure if the schemes $\mathcal{E}_2$ and $\mathcal{H}$ are secure (cf. Theorem 3 in [3]).

7 Bridges from circuits and Micciancio's Theorem

In this section we explain how a bridge can be canonically associated to a pair consisting of an encryption scheme and a circuit that can be homomorphically evaluated. As a consequence, one can translate every discussion about homomorphic circuit evaluation and composition of circuits into the language of bridges developed here and in [3]. Moreover, one can see Theorem 3 as a generalisation of the following theorem:

Theorem 5 (Micciancio). *Every circular secure FHE encryption scheme* $\mathcal{H} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec}, \mathrm{Eval})$*, can be transformed into a secure fully composable homomorphic encryption scheme* $\mathcal{H}' = (\mathrm{KeyGen}', \mathrm{Enc}, \mathrm{Dec}, \mathrm{Eval}')$.

The terminology *fully composable* is clarified in Definition 10 below. A sketch of the proof of this theorem can be found in the talk [27] [4]. The idea of the proof is to use a procedure similar to the one in Gentry-type bridge construction. We saw in Theorem 3 that these give rise to complete bridges. The difference between the Gentry-type bridge construction and Micciancio's resides in the KeyGen algorithms. In the key generation process of a Gentry type bridge, it is required that the keys of the second scheme are generated independently from the keys of the first one. On the other hand, in Micciancio's construction the two schemes have identical secret and public keys. This difference impacts only the security of the bridge and does not affect its completeness property. This can give rise to security issues for which one is forced to add an extra assumption, namely the circular security assumption.

We start by showing how one can associate bridges to circuits and homomorphic encryption schemes.

Let $\mathcal{E} = (\mathrm{KeyGen}, \mathrm{Enc}, \mathrm{Dec})$ be an encryption scheme and let $C : \mathcal{M}^r \to \mathcal{M}$ be a boolean circuit defined over the plaintext $\mathcal{M}$ of $\mathcal{E}$.

Assume that the scheme $\mathcal{E}$ is $C-$homomorphic. Recall that a scheme is homomorphic with respect to the circuit C, or is $C-$homomorphic, if there exists an algorithm $\mathrm{Eval}(evk, C, c_1, \dots c_r)$ which takes as input an evaluation key evk, the circuit C, and an element of $\mathcal{C}^r$ such that the outputted ciphertext satisfies the following correctness condition:

$$\mathrm{Dec}(sk, \mathrm{Eval}(evk, C, \mathrm{Enc}(m_1), \dots, \mathrm{Enc}(m_r))) = C(m_1, \dots, m_r),$$

for all $(m_1, \dots, m_r) \in \mathcal{M}^r$.

In this context, we associated to the pair $(\mathcal{E}, C)$, the bridge $\mathbf{B}_C : \mathcal{E}^{(r)} \to \mathcal{E}$ where the function ι is given by:

$$\iota(m_1, \dots, m_r) := C(m_1, \dots, m_r),$$

the bridge key bk consists of the evaluation key evk (possibly empty), and the bridge algorithm is

[4] This is a talk given by D. Micciancio at the FHE.org conference 2022, that took place in Trondheim, NO - an affiliated event to the Eurocrypt 2022 conference. The proof starts at time 25:39.

$$f_C(bk, c_1, \ldots, c_r) := \mathrm{Eval}(evk, C, c_1, \ldots, c_r).$$

One can easily see that the correctness property of Eval guarantees that the above construction is indeed a bridge. Moreover, this bridge is secure as long as the C-homomorphic scheme $\mathcal{E}$ is secure.

Remark 8. If $\mathcal{E}$ is an FHE scheme, the above procedure gives rise to a family of bridges $\mathbf{B}_C$, one for each boolean circuit C. By concatenating such bridges $\mathbf{B}_{C_1}, \ldots, \mathbf{B}_{C_s} : \mathcal{E}^{(r)} \to \mathcal{E}$, one obtains a bridge $\mathbf{B}_{C_1,\ldots,C_s} : \mathcal{E}^{(r)} \to \mathcal{E}^{(s)}$.

In his talk [27], Micciancio points out one foundational problem in the definition of a fully homomorphic encryption scheme. Namely, the definition of an FHE scheme does not guarantee correct decryption if one sequentially evaluates two (multivalued) circuits on encrypted data. This issue is an instance of the more general problem of composing bridges.

More precisely, suppose bridges $\mathbf{B}_{C_1,\ldots,C_s} : \mathcal{E}^{(r)} \to \mathcal{E}^{(s)}$ and $\mathbf{B}_{D_1,\ldots,D_t} : \mathcal{E}^{(s)} \to \mathcal{E}^{(t)}$ are constructed as above, for some FHE scheme $\mathcal{E}$. The issue raised by Micciancio is equivalent to the composability of the pair of bridges $(\mathbf{B}_{C_1,\ldots,C_s}, \mathbf{B}_{D_1,\ldots,D_t})$ (see Definition 8) for all such circuits.

We recall the following definition due to Micciancio.

Definition 10. *An encryption scheme $\mathcal{E}$ is called* fully composable encryption scheme [5] *(FcHE) if for any circuit $C : \mathcal{M}^r \to \mathcal{M}$, the following relation*

$$\mathrm{Dec}(sk, \mathrm{Eval}(evk, C, c_1, \ldots, c_r)) = C(\mathrm{Dec}(sk, c_1), \ldots, \mathrm{Dec}(sk, c_r))$$

holds for all $c_1, \ldots, c_r \in \mathcal{C}$.

Remark 9. It is an immediate consequence of the definition that a scheme is fully composable if and only if every bridge $\mathbf{B}_C$ from the familly defined above is a complete bridge (see Definition 6).

We point out the following immediate consequence, which is consistent with the terminology chosen by Micciancio.

Proposition 3. *Let $\mathcal{E}$ be an FcHE scheme and let C_1, C_2 be two (multivalued) circuits, $C_1 : \mathcal{M}^r \to \mathcal{M}^s$ and $C_2 : \mathcal{M}^s \to \mathcal{M}^t$. Then*

$$\mathrm{Dec}(sk, \mathrm{Eval}(evk, C_2, \mathrm{Eval}(evk, C_1, c_1, \ldots, c_r)) = C_2(C_1(m_1, \ldots, m_r))$$

for all $c_1, \ldots, c_r \in \mathcal{C}$, where $m_i = \mathrm{Dec}(sk, c_i)$ for all $i = \overline{1, r}$.

In particular, in FcHE schemes, one can homomorphically compose [6] any circuits. However, the converse is not true:

[5] This is the name coined by Micciancio, based on the consequence of this property described bellow. We chose to use the name complete for its generalisation to bridges.

[6] By homomorphic composition we understand sequential evaluation of two (multivalued) circuits on encrypted data.

Example 5. Consider any FHE scheme $\mathcal{E}$ which is constructed using a bootstrapping procedure and such that for every ciphertext c, we have $\text{Bootstrap}(c) \in \text{Enc}(pk, \text{Dec}(sk, c))$. In such a scheme, one can homomorphically perform bootstrapping after every operation. Then modify the evaluation algorithm of $\mathcal{E}$ such that for every circuit C,

$$\text{Eval}'(evk, C, c_1, \ldots, c_r) := \text{Bootstrap}(\text{Eval}(evk, C, c_1, \ldots, c_r)).$$

In such a scheme, one can homomorphically compose every two circuits, as the output of every evaluation algorithm will be a fresh encryption. However, such a scheme is not necessarily a FcHE scheme according to the Definition 10.

We obtain Micciancio's result as a corollary to Theorem 3, as we now explain. Indeed, recall from the construction of Gentry-type bridges that one can realise the set of secret keys of $\mathcal{H}$ and its ciphertext space as subsets of $\mathcal{M}^e$ and respectively $\mathcal{M}^n$, where $\mathcal{M}$ is the plaintext of $\mathcal{E}$. In the same section, we constructed the map $\widetilde{\text{Dec}} : \mathcal{M}^e \times \mathcal{M}^n \to \mathcal{M}$. For any ciphertext c of $\mathcal{H}$, we can restrict the second argument of $\widetilde{\text{Dec}}$ to obtain $\widetilde{\text{Dec}}(\cdot, c) : \mathcal{M}^e \to \mathcal{M}$.

The encryption scheme $\mathcal{H}'$ proposed by Micciancio is constructed as follows. The encryption and decryption procedures are the ones from $\mathcal{H}$. The key generation algorithm uses KeyGen to obtain a triple (sk, pk, evk). The algorithm now encrypts each component of $sk = (sk[1], ..., sk[e])$, viewed as an element of $\mathcal{M}^e$, to obtain $(\widetilde{sk[1]}, ..., \widetilde{sk[e]}) \in \mathcal{C}^e$. Finally, it outputs the triple (sk, pk, evk'), where $evk' = (evk, \widetilde{sk[1]}, ..., \widetilde{sk[e]})$.

For any $C : \mathcal{M}^l \to \mathcal{M}$, the evaluation algorithm Eval' works as follows. Let $c_1, c_2, \ldots, c_l \in \mathcal{C} \subseteq \mathcal{M}^n$ be any l ciphertexts. Let $g_{(C,c_1,\ldots,c_l)} : \mathcal{M}^e \to \mathcal{M}$ be defined as

$$g_{(C,c_1,\ldots,c_l)}(sk) = C(\widetilde{\text{Dec}}(sk, c_1), \widetilde{\text{Dec}}(sk, c_2), \ldots, \widetilde{\text{Dec}}(sk, c_l)).$$

The evaluation algorithm of $\mathcal{H}'$ is given by:

$$\text{Eval}'(evk', C, c_1, ..., c_l) := \text{Eval}(evk, g_{(C,c_1,\ldots,c_l)}, \widetilde{sk[1]}, ..., \widetilde{sk[e]}).$$

We now use the language of bridges to show that $\mathcal{H}'$ is a secure FcHE, under the circular security assumption for $\mathcal{H}$.

The circuit C gives rise as above to a bridge

$$\mathbf{B}_C : \mathcal{H}'^{(l)} \to \mathcal{H}'.$$

Since $\mathcal{H}$ and $\mathcal{H}'$ are identical once we forget the evaluation algorithms, we can view this bridge as a bridge $\mathbf{Br}_C : \mathcal{H}^{(l)} \to \mathcal{H}$. However, this bridge is *not* the bridge associated to the circuit C as above. Actually, it is easy to see that this bridge is the Gentry-type bridge constructed in Section 6 where $\mathcal{E} = \mathcal{H}^{(l)}$, and $\iota : \mathcal{M}^l \to \mathcal{M}$ is defined by C, with the difference that the KeyGen outputs the same secret key for both $\mathcal{E}$ and $\mathcal{H}$. However, the proof of Theorem 3 transports identically, thus the bridge $\mathbf{B}_C$ is complete. Using Remark 9, the scheme $\mathcal{H}'$ is an FcHE scheme.

As we mentioned in Remark 7, the authors proved in [3, Theorem 3] that any Gentry-type bridge between two secure encryption schemes is also secure. However, this result does not directly apply to $\mathbf{B}_C$ because this bridge has a slightly different KeyGeneration algorithm. Namely, here the secret keys of the encryption schemes involved in the bridge are identical, whereas in Gentry-type bridges they are generated independently. In the present situation, the security analysis of the scheme $\mathcal{H}'$ is much simpler, because it is equivalent to the security analysis of $\mathcal{H}[evk']$. On the other hand, the security of the latter scheme reduces to the circular security assumption.

References

1. Ateniese, G., Fu, K., Green, M., Hohenberger, S.: Improved proxy re-encryption schemes with applications to secure distributed storage, In: ACM Trans. Inf. Syst. Secur., vol 9, no 1, 1–30 (2006)
2. Barcau, M., Paşol, V., Pleşca, C.: Monoidal Encryption over $\mathbb{F}_2$, In: Lanet JL., Toma C. (eds) Innovative Security Solutions for Information Technology and Communications, SECITC 2018, LNCS, vol 11359, pp. 504–517, Springer, Cham (2019).
3. Barcau, M., Lupaşcu, C., Paşol, V., Ţurcaş G. C.: Bridges connecting Encryption Schemes, In Bella, G., Doinea, M., Janicke, H. (eds) Innovative Security Solutions for Information Technology and Communications. SecITC 2022. LNCS, vol 13809, pp. 37–64, Springer, Cham (2023).
4. Bellare, M., Rogaway, P., *Introduction to Modern Cryptography*, University of California, Notes, `https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf`.
5. Boura, C., Gama, N., Georgieva, M., Jetchev, D.: CHIMERA: Combining Ring-LWE-based Fully Homomorphic Encryption Schemes, Journal of Mathematical Cryptology **14**(1), pp. 316 – 338 (2020).
6. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping, ACM Transactions on Computation Theory **6**(3), No. 13, pp. 1–36 (2014).
7. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE, `http://eprint.iacr.org/2011/34`.
8. Dodis, Y., Ivan, A.: Proxy cryptography revisited, In: Proceedings of the Tenth Network and Distributed System Security Symposium, February 2003.
9. Phong, L. T., Wang, L., Aono, Y., Nguyen, M. H., Boyen, X.:Proxy Re-Encryption Schemes with Key Privacy from LWE, `https://eprint.iacr.org/2016/327.pdf`
10. Canetti, R., Krawczyk, H.: Universally composable notions of key exchange and secure channels., In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 337–351. Springer, Heidelberg (2002).
11. Canetti, R., Dodis, Y., Pass, R., Walfish, S.: Universally Composable Security with Global Setup, In: Vadhan, S.P. (eds) Theory of Cryptography. TCC 2007. Lecture Notes in Computer Science, vol 4392. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-70936-7-4
12. Canetti, R.: Universally Composable Security, Journal of the ACM, **67**5, 2020, pag 1–94
13. Castagnos, G., Imbert, L., Laguillaumie, F.: Encryption Switching Protocols Revisited: Switching Modulo p, In: Katz J., Shacham H. (eds) Advances in Cryptology, CRYPTO 2017, LNCS, vol. 10401, pp. 255 – 287, Springer, Cham (2017).

14. Cohen, A.: What About Bob? The Inadequacy of CPA Security for Proxy Reencryption, PKC (2) 2019, pp. 287–316.
15. certSIGN RD: CSGN GitHub repository, https://github.com/certFHE/CSGN. Last accessed on 20 May 2021.
16. Couteau, G., Peters, T., Pointcheval, D.: Encryption Switching Protocols, In: Robshaw M., Katz J. (eds) Advances in Cryptology, CRYPTO 2016, LNCS, vol. 9814, pp. 308 – 338. Springer, Berlin, Heidelberg (2016).
17. Dobraunig, C., Eichlseder, M., Grassi, L., Lallemand, V., Leander, G., List, E., Mendel, F., Rechberger, C.: Rasta: A Cipher with Low ANDdepth and Few ANDs per Bit, In: Advances in Cryptology, CRYPTO 2018, LNCS, vol. 10991, pp. 662 – 692. Springer, Cham (2018).
18. Dobraunig, C., Grassi, L., Helminger, L., Rechberger, C., Schofnegger, M. and Walch, R.: Pasta: A Case for Hybrid Homomorphic Encryption. In Cryptology ePrint Archive (2021).
19. Dottling, N., Nishimaki, R.: Universal Proxy Re-Encryption, Cryptology ePrint Archive, Report 2018/840, to appear in PKC '21.
20. Ducas, L., Micciancio, D.: FHEW: Bootstrapping Homomorphic Encryption in Less Than a Second, Advances in Cryptology - EUROCRYPT 2015, Lecture Notes in Computer Science vol. 9056, pp. 617 – 640.
21. Gentry, C: A fully homomorphic encryption scheme, PhD thesis, Stanford University, 2009.
22. Gentry, C.: Computing arbitrary functions of encrypted data, Communications of the ACM, **53**(3), pp. 97 – 105 (2010).
23. Gentry C., Halevi S., Smart N.P.: Homomorphic Evaluation of the AES Circuit. In: Safavi-Naini R., Canetti R. (eds) Advances in Cryptology, CRYPTO 2012, LNCS, vol. 7417, pp. 850–867. Springer, Berlin, Heidelberg (2012).
24. Goldreich, O.: A note on computational indistinguishability, Information Processing Letters, **34**(6), pp. 277 – 281.
25. Goldwasser, S., Micali, S.: Probabilistic encryption and how to play mental poker keeping secret all partial information, In: STOC '82: Proceedings of the fourteenth annual ACM symposium on Theory of computing, pp. 365 – 377. Association for Computing Machinery, New York, NY (1982).
26. Lee, Y. et al. (2023): Efficient FHEW Bootstrapping with Small Evaluation Keys, and Applications to Threshold Homomorphic Encryption, In: Hazay, C., Stam, M. (eds) Advances in Cryptology, EUROCRYPT 2023. LNCS, vol. 14006, Springer, Cham (2023).
27. Micciancio, D., [FHE_org], (9th of June, 2022), Fully Homomorphic Encryption: Definitional issues and open problems [Video], Youtube, `https://www.youtube.com/watch?v=b24WJyS0dmg`
28. Micciancio, D., Polyakov, Y.: Bootstrapping in FHEW-like Cryptosystems, In: Proceedings of the 9th on Workshop on Encrypted Computing & Applied Homomorphic Cryptography (WAHC '21). Association for Computing Machinery, New York, NY, USA, 17—28.
29. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, In: Gabow, H.N., Fagin, R., (eds.), 37th ACM STOC, pp. 84 – 93. ACM Press, May (2005).
30. Sander, T., Young, A., Yung, M.: Non-Interactive CryptoComputing For NC^1. In: FOCS '99: Proceedings of the 40th Annual Symposium on Foundations of Computer Science, pp. 554 – 566, IEEE Computer Society, NW Washington, DC, United States (1999).
31. Smart, N.: Cryptography Made Simple, Springer, Cham (2016).