Cryptanalysis of Ring Homomorphic Encryption Schemes

Mugurel Barcau[1,2], Vicenţiu Paşol[1,2]

[1] certSIGN - Research and Development, Bucharest, Romania
[2] Institute of Mathematics "Simion Stoilow" of the Romanian Academy
mugurel.barcau@imar.ro, vicentiu.pasol@imar.ro

Abstract. We analyze the structure of finite commutative rings with respect to its idempotent and nilpotent elements. Based on this analysis we provide a *quantum-classical* IND-CCA[1] attack for ring homomorphic encryption schemes. Moreover, when the plaintext space is a finite reduced ring, i.e. a product of finite fields, we present a key-recovery attack based on representation problem in black-box finite fields. In particular, if the ciphertext space has smooth characteristic the key-recovery attack is effectively computable. We also extend the work of Maurer and Raub on representation problem in black-box finite fields to the case of a black-box product of finite fields of equal characteristic.

1 Introduction

One of the most important problems in cryptography is the construction of an efficient and secure fully homomorphic encryption (FHE) scheme. A practical solution to this problem would have a large number of consequences, such as computation on encrypted data held on an untrusted server. In [16], C. Gentry came up with the first construction of such a scheme based on ideal lattices. Gentry's approach goes as follows: first, he constructs a somewhat homomorphic encryption scheme which is an encryption scheme that supports evaluating low-degree polynomials on the encrypted data; next, he "squashes" the decryption procedure so that it can be expressed as a low-degree polynomial which is supported by the scheme; and finally, he develops a bootstrapping technique which allows one to obtain a fully homomorphic scheme. The first generation of fully homomorphic encryption schemes ([17], [14], [33], [13], [19]) was constructed following Gentry's recipe. A second generation of encryption schemes started in [7], where fully homomorphic encryption was established in a simpler way, based on the learning with errors assumption; the scheme was then improved in [9]. Currently, perhaps the simplest FHE scheme based on the learning with errors assumption is by Brakerski [8] who builded on Regev's public key encryption scheme [29]. The most recent achievement in this direction was obtained in [20], where a significant FHE scheme was introduced claiming three important properties: simpler, faster, and attribute-based FHE. Another very recent approach aiming for producing FHE was presented in [15], where the authors based their construction on the finite field isomorphism problem. All these schemes are based on the method of constructing a noisy version of the ciphertext(the noise is added to guarantee the security of the cryptosystem). The output of this approach is called noisy FHE scheme. In this respect, an important and natural question would be whether one can actually construct a noise-free FHE scheme. A possible approach towards noise-free FHE scheme, could be the following setting: the ciphertext space and the plaintext space both have ring structures, and the decryption algorithm is a ring homomorphism, so that one would call such a scheme a ring homomorphic encryption scheme. Let us mention here that a different approach towards achieving noise-free FHE was considered in [27]. Namely, they showed that the NAND operator, which is sufficient for constructing arbitrary operations on bits, can be realized (in a certain suitable sense) in some non-commutative groups.

In this article, we investigate the structure of ring homomorphic encryption schemes and their security, where the ciphertext and plaintext spaces are finite commutative non-unital black-box rings.

1.1 Our Contribution

The contribution of this work is threefold. First, we prove that any ring homomorphic encryption scheme with commutative ciphertext and plaintext spaces are not secure against quantum adversaries, where quantum computing is required only in the first phase of the attacks, when the "secret key" is computed. More precisely, we show that any ring homomorphic encryption scheme over a quasi-unital ring (see section 3) is not IND-CCA^1-secure. Moreover, in the case of a ring homomorphic encryption scheme whose plaintext space is a reduced ring we present a key-recovery attack based on the representation problem in black-box finite fields ([25]). In particular, if the characteristic of the ciphertext space is smooth then our key-recovery attack is effectively computable. These results are proved under the assumption that the ciphertext and plaintext spaces are black-box rings (see definition 5). In particular, we assume that a finite set of generators is known both for the ciphertext space and for the plaintext space. To prove these results, a big part of the paper is devoted to the computation of primitive idempotents of finite commutative black-box rings. This is the second important contribution of this work. In the end, we show that the results in [25] can be extended to the case of a product of finite fields of equal characteristic.

1.2 Related Work

The security of the known (noisy) FHE schemes, was considered in many papers, among which we mention [10] and [23]. It has been shown that these schemes are not IND-CCA^1 secure. On the other hand, to our knowledge, the security of ring homomorphic encryption schemes was considered only in [5], where the security of ring homomorphic encryption schemes over $\mathbb{F}_2$ has been investigated. However, there exists a result that is related to our work, as we shall explain. It is clear that any ring homomorphic encryption scheme gives rise to a (commutative) group homomorphic encryption scheme by forgetting the multiplicative structure on both the ciphertext and plaintext spaces. In [1], an IND-CPA attack is presented on commutative group homomorphic encryption schemes. This attack may be used in the case of a ring homomorphic encryption scheme, but is much less efficient than our attack. Indeed, the attack is based on the existence of a set of generators for the ciphertext space, viewed as an abelian group (or as a $\mathbb{Z}$-module). Our IND-CCA^1 attack is also based on the existence of a set of generators of the ciphertext space, but viewed as a ring (or as a $\mathbb{Z}$-algebra). In many situations in public key cryptography, the rings that represent ciphertext spaces are described using generators and (possible hidden) relations, so that our assumption is not too restrictive. Moreover, the existence of a finite set of generators of a certain $\mathbb{Z}$-algebra R, may produce a finite set of generators (see [3]) for the $\mathbb{Z}$-module $(R, +)$, but the size of this set of generators is much larger than the size of the initial one, so that the algorithm in [1] is less efficient. In addition, in a general enough setting we propose key-recovery attacks, which obviously is a much stronger attack than IND-CCA^1. Moreover, we use quantum algorithms only for the computation of the "secret key"(which in the case of a IND-CPA/CCA attack corresponds to the first phase of the attack) and then we decrypt any ciphertext using classic algorithms, which is not the case for the attack presented in [1] where in both phases of the attack one needs to use quantum computations. One can adapt the arguments in this work to construct IND-CPA attacks for the ring homomorphic encryption schemes using the idea of δ-coverings described in [1]. However, for the clarity of the ideas presented in this paper we decided to analyze only the IND-CCA^1 security.

1.3 Outline

In the next section we present the notations and definitions of ring homomorphic encryption schemes and security attacks. In Section 3 we prove that any finite commutative ring has a unique decomposition as a product of a unital ring and a nilpotent ring (Theorem 1) and provide an explicit projection to its unital part. The unital part decomposes further as a product of local unital rings (Artin's decomposition theorem [4]), each component corresponding to a primitive idempotent. We then prove that any nontrivial homomorphism from a unital ring to a finite local ring factorizes through a unique projection to one of its local components. This fact will be essential in constructing our attacks. In section 4 we recall the quantum algorithm for computing associated idempotents of elements of black-box semigroups, and we also show that in a finite ring of prime power characteristic this quantum algorithm may be replaced by a classical one. Section 5 is devoted to the computational aspects of the structural decomposition of rings, presented previously. More precisely, we present algorithms that compute the primitive idempotents of a ring and the residue fields of its local components. In section 6 we provide two algorithms: an IND-CCA^1 attack on ring homomorphic encryption schemes over general quasi-unital rings, and a key-recovery attack on ring homomorphic encryption schemes over reduced rings, based on the solvability of the representation problem problem in black-box finite fields. Also, we extend the results of [25] to the case of a product of finite fields of equal characteristic.

2 Homomorphic Encryption - Definitions

The homomorphic encryption schemes in their generality were treated by different authors and many treaties. We refer to [21] and [31] for a comprehensive treatment of the subject and also to [2] for a treatment of their security behavior. Let us define ring homomorphic encryption schemes and explore their properties. Throughout this section (and this work) we use λ to indicate the security parameter. Since a ring homomorphic encryption scheme is a certain type of homomorphic encryption scheme, we introduce first this concept.

Definition 1. *A homomorphic (public-key) encryption scheme*

$$\boldsymbol{HE} = (\boldsymbol{HE.KeyGen}, \boldsymbol{HE.Enc}, \boldsymbol{HE.Dec}, \boldsymbol{HE.Eval})$$

is a quadruple of PPT algorithms as follows:

- **Key Generation.** *The algorithm $(pk, evk, sk) \leftarrow \boldsymbol{HE.KeyGen}(1^\lambda)$ takes a unary representation of the security parameter and outputs a public encryption key pk, an evaluation key evk, and a secret decryption key sk.*
- **Encryption.** *The algorithm $c \leftarrow \boldsymbol{HE.Enc}_{pk}(m)$ takes the public key pk and a single message m and outputs a ciphertext c.*
- **Decryption.** *The algorithm $m^\star \leftarrow \boldsymbol{HE.Dec}_{sk}(c)$ takes the secret key sk and a ciphertext c and outputs a message $m^\star$.*
- **Homomorphic Evaluation.** *The algorithm $c_f \leftarrow \boldsymbol{HE.Eval}_{evk}(f, c_1, ..., c_\ell)$ takes the evaluation key evk, a boolean circuit $f : \{0,1\}^\ell \to \{0,1\}$ and a set of ℓ ciphertexts $c_1, ..., c_\ell$, and outputs a ciphertext c_f.*

We say that a scheme **HE** is *$\mathcal{C}$-homomorphic* for a class of circuits $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$, if for any sequence of circuits $f_\lambda \in \mathcal{C}_\lambda$ and respective inputs $\mu_1, ..., \mu_\ell \in \{0,1\}$ (where $\ell = \ell(\lambda)$), it holds that

$$\Pr[\mathbf{HE.Dec}_{sk}(\mathbf{HE.Eval}_{evk}(f_\lambda, c_1, ..., c_\ell) \neq f_\lambda(\mu_1, ..., \mu_\ell)] = \mathrm{negl}(\lambda),$$

where $(pk, evk, sk) \leftarrow \mathbf{HE.KeyGen}(1^\lambda)$ and $c_i \leftarrow \mathbf{HE.Enc}_{pk}(\mu_i)$.

In addition, we say that a homomorphic scheme **HE** is *compact*, if there exist a polynomial $s = s(\lambda)$ such that the output length of **HE.Eval** is at most s bits long, regardless of f or the number of inputs.

Definition 2. *A homomorphic scheme **HE** is fully homomorphic (**FHE**) if it is compact and homomorphic for the class of all circuits.*

Remark 1. If one weakens the compactness condition, one can construct such schemes as in [6].

In this work we will consider only the following type of **HE** schemes:

Definition 3. *A ring homomorphic encryption scheme (**RHE**) is a family indexed by λ of quadruples $(R_\lambda, S_\lambda, \mathbf{Enc}_\lambda, \mathbf{Dec}_\lambda)$, consisting of finite rings R_λ, S_λ, a homomorphism of rings $\mathbf{Dec}_\lambda(sk, \cdot) : R_\lambda \to S_\lambda$, and a PPT algorithm $R_\lambda \ni c \leftarrow \mathbf{Enc}_\lambda(pk, m)$, where $m \in S_\lambda$ such that the following conditions hold:*

1. *$\mathbf{Dec}_\lambda(sk, c) = m$, for any $c \leftarrow \mathbf{Enc}_\lambda(pk, m)$,*
2. *the scheme is compact as a homomorphic encryption scheme.*

Let us note that compactness is equivalent in this case to the existence of two representations: $R_\lambda \overset{\imath_R}{\hookrightarrow} \{0,1\}^{n_R(\lambda)}$, $S_\lambda \overset{\imath_S}{\hookrightarrow} \{0,1\}^{n_S(\lambda)}$, where $n_R(\lambda), n_S(\lambda)$ are polynomial in the security parameter λ, such that $\mathbf{Dec}_\lambda : \imath_R(R_\lambda) \to \imath_S(S_\lambda)$ is a deterministic polynomial time algorithm, and $\mathbf{Enc}_\lambda : \imath_S(S_\lambda) \rightsquigarrow \imath_R(R_\lambda)$ is a probabilistic polynomial time algorithm. Hereafter, we will assume that the finite rings R_λ and S_λ, i.e. the ciphertext and plaintext spaces of a ring homomorphic encryption scheme, are commutative rings, not necessarily unital, unless otherwise specified.

Remark 2. If the plaintext space is a quasi-unital ring(see section 3), then a ring homomorphic encryption scheme is a fully homomorphic encryption scheme. Indeed, by Theorem 1 and Proposition 1 the plaintext space S_λ contains a non-zero idempotent, so that one can construct an $\mathbb{F}_2$-structure inside S_λ. To show that such a ring homomorphic encryption scheme is a fully homomorphic encryption scheme, one replaces any gate of a boolean circuit with the corresponding small degree polynomial and use the homomorphicity of the decryption map.

We briefly recall the only security notion we need in what follows, that is indistinguishability under chosen-ciphertext attack (IND-CCA^1) for public key encryption schemes. To define it we introduce first the following two-phase experiment in which $\mathcal{A}$ is a polynomial time adversary.

Experiment IND-CCA^1
- Phase One: Generate a pair of keys $(pk, sk) \leftarrow \mathbf{HE.KeyGen}(1^\lambda)$. Give $\mathcal{A}$ access to a decryption oracle and run $\mathcal{A}$ on input pk. $\mathcal{A}$ proposes two messages m_0 and m_1.
- Phase Two: Choose at random a bit i, and compute $c \leftarrow \mathbf{HE.Enc}_{pk}(m_i)$. Give c to $\mathcal{A}$, and let $\mathcal{A}$ continue its computation without access to the decryption oracle.
- Let m' be $\mathcal{A}$'s output. Output 1 if $m' = m_i$ and 0 otherwise.

Definition 4. *A scheme **HE** is IND-CCA^1 secure if for any polynomial time adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ satisfies:*

$$Adv_{IND\text{-}CCA^1}(\mathcal{A}) := \left| Pr\left[IND\text{-}CCA^1(\mathcal{A}) = 1\right] - \frac{1}{2} \right| = negl(\lambda).$$

We shall also say that a scheme is *quantum-classical* IND-CCA^1 secure if the adversary $\mathcal{A}$ is allowed to use classical and quantum algorithms in the first phase, whereas in the second phase the adversary is allowed to use only classical algorithms. In the same manner, one can define quantum-quantum IND-CCA[1] security etc..

In what follows, we shall suppose that the ciphertext space of a ring homomorphic encryption scheme is a black-box ring. We give a formal definition of this notion:

Definition 5. *A ring oracle OR_λ takes queries of the form $(\lambda, x, y, +)$, $(\lambda, x, -)$, $(\lambda, 0)$, $(\lambda, x, y, \cdot)$, where x, y are strings of length $n(\lambda)$ (polynomial in λ) over $\{0,1\}$. The response to each of these queries is either a string of length $n(\lambda)$ or a symbol indicating invalid query. Let $OR(\lambda)$ be the set of $x \in \{0,1\}^{n(\lambda)}$ for which $(\lambda, x, -)$ is a valid query (the response to this query is the string encoding the additive inverse of x, and the response to $(\lambda, 0)$ is the string encoding additive identity). We say that OR_λ is a ring oracle if, for each λ, $OR(\lambda)$ is either empty or a ring with ring operations described by the responses to the above queries. The subrings of $OR(\lambda)$, given by finite generating sets will be called black-box rings, or BBR for short.*

Remark 3. By a finite generating set of a (nonunital) ring R, we understand a finite subset $\{g_1, g_2, ..., g_d\}$ of R such that any element of the ring can be written in the form $P(g_1, g_2, ..., g_d)$, where $P(X_1, ..., X_d) \in \mathbb{Z}[X_1, ..., X_d]_+$, i.e. $P(0, ..., 0) = 0$. If R is a unital ring, then the unity itself can be written as a polynomial with integer coefficients in the set of generators, so that, in this case, $\{g_1, g_2, ..., g_d\}$ is a generating set for R if any element of the ring can be written in the form $P(g_1, g_2, ..., g_d)$, where $P(X_1, ..., X_d) \in \mathbb{Z}[X_1, ..., X_d]$.

3 Finite Commutative Rings

In this section we investigate the structure of (non-unital) finite commutative rings. Some of the results are known to specialists, but since we couldn't find them in the literature in the explicit form we need for our applications, we shall give all the necessary details. We have the following structural theorem :

Theorem 1. *Any finite commutative ring is isomorphic to a product of a unital ring and a nilpotent ring. Moreover, the decomposition is unique (up to isomorphism).*

A commutative ring R is called *nilpotent* if there exist a positive integer n such that $R^n = \{0\}$. In the case of a finite commutative ring R, this is equivalent to the existence, for any $x \in R$, of a positive integer (that may depend on x), such that $x^n = 0$. We say that a finite commutative ring is *quasi-unital* if it is not nilpotent, in other words its unital part is non-trivial.

We shall prove this theorem by explicitly describing this decomposition (inside the ring), while the unicity comes from the properties of its pieces: unital, respectively nilpotent. The reader should be warned of the fact that the nilpotent ring exhibited in this theorem is also an ideal of the ring, but, in general, is *not* the nilpotent radical of the ring. It is rather the maximal nilpotent ideal of the ring, which is an internal direct summand as an ideal. The constructive nature of our proof allows us to find a computable description of the structure of finite commutative rings; this being essential in constructing our attacks on ring homomorphic encryption schemes.

3.1 The Idempotent $\mathbb{F}_2$-algebra of R

If R is a ring then we denote by $E(R)$ the idempotent semigroup associated to the semigroup $(R, \cdot)$. If we define addition in $E(R)$ by: $e \oplus e' = e + e' - 2ee'$, $\forall e, e' \in E(R)$, then this becomes a ring of characteristic 2. We shall refer to this ring $(E(R), \oplus, \cdot)$ as being the idempotent ring of R, or as the idempotent $\mathbb{F}_2$-algebra of R. It is shown in [5], that if R is a finite ring then there is a well defined map $R \to E(R)$, that is a homomorphism of multiplicative semigroups. Then:

Proposition 1. *Let R be a (non-unital) finite commutative ring and let $E(R)$ be its idempotent ring then:*

i) $E(R)$ is an $\mathbb{F}_2-$algebra and is isomorphic to $\mathbb{F}_2^n$ for some n.

ii) Any nontrivial ring homomorphism $\phi : E(R) \to \mathbb{F}_2$ is the projection on the i-th coordinate, for some $i \in \{1, ..., n\}$ (here we identify $E(R)$ with $\mathbb{F}_2^n$ via the above isomorphism).

For a proof of this proposition see [5], Proposition 4.

Remark 4. If R is a finite commutative ring *with unity* then it is an Artin ring, and the structure theorem for Artin rings (Theorem 8.7 in [4]) asserts that R is isomorphic to a product $R_1 \times ... \times R_n$ of local Artin rings. This isomorphism gives rise to

$$E(R) \simeq E(R_1 \times ... \times R_n) \simeq \mathbb{F}_2^n$$

The proof of the last proposition shows that even in the case of a non-unital ring R, the idempotent algebra is isomorphic to $\mathbb{F}_2^n$. Notice that if R is a ring with unity, then $1 = e_1 + ... + e_n$, where $e_1, ..., e_n$ are the primitive idempotents of R. Therefore, the map $R \to \prod Re_i$, $x \mapsto (xe_1, ..., xe_n)$ is an isomorphism, so that the rings R_i are in fact isomorphic to the rings Re_i. In particular, the number of local Artin rings that appear in the decomposition of R is equal to the number of its primitive idempotents (for more details see [5]).

In the next section, we shall use the structure of the idempotent $\mathbb{F}_2$-algebra to give an explicit proof of Theorem 1.

3.2 Explicit Version of Theorem 1

Theorem 2. *Let R be a finite commutative ring and let $e_1, ..., e_n$ be its primitive idempotents. Let $\bar{e} = \bar{e}_R := e_1 \oplus ... \oplus e_n$, $\bar{R} := R \cdot \bar{e}$, and $N_R := \{x \in R \mid x\bar{e} = 0\}$. Then:*

1. *$\bar{R}$ is a unital subring, and N_R is a nilpotent ideal, hence subring of R.*
2. *$R \simeq \bar{R} \times N_R$, where $x \mapsto (x\bar{e}, x - x\bar{e})$.*
3. *Any morphism of rings $S \to R$ with S unital, factors as $S \to \bar{R} \subseteq R$.*

Proof. 1. The fact that $\bar{R}$ is a unital ring is clear. The unit is $\bar{e}$, because $x\bar{e}\cdot\bar{e} = x\bar{e}$, $\forall x \in R$. The following equality $x \cdot \bar{e} = 0$ yields $x^n \cdot \bar{e} = 0$ for any positive integer n, so that $e(x) \cdot \bar{e} = 0$. But now the identity takes place in $\bar{R}$ where $\bar{e}$ is the unit, thus $e(x) = 0$, so that x is nilpotent.

2. It is an easy exercise to check that the map $\mu : R \to \bar{R} \times N_R$ defined by $\mu(x) := (x\bar{e}, x - x\bar{e})$ is indeed a ring homomorphism. It is an isomorphism of rings, its inverse being $\mu^{-1}(a, b) := a + b$.

3. See the proof of the next remark.

Remark 5. The map $R \mapsto \bar{R}$ is a functor from $CRngs$, that is the category of commutative rings not necessarily with unity, to its full subcategory $\overline{CRings}$ consisting of commutative rings with unity, but here the morphisms may not be unital homomorphisms, as in the case of $CRings$, the category of commutative rings with unity and unital homomorphisms of rings as morphisms. More precisely, it is the right adjoint functor of the forgetful functor $\overline{CRings} \to CRngs$, given by forgetting the multiplicative identity. In particular, the above decomposition is not only unique, it is also functorial.

To prove that $R \mapsto \bar{R}$ is the right adjoint of the forgetful functor, consider a morphism of crngs $\phi : S \to R$ such that $S \in \overline{CRings}$. Notice that $e := \phi(1_S)$ is an idempotent of R. Then $\phi(x) = \phi(1_S \cdot x) = \phi(1_S) \cdot \phi(x) = e \cdot \phi(x) = \bar{e} \cdot e \cdot \phi(x) \in \bar{R}$. Hence the morphism factors through $\bar{R} \hookrightarrow R$.

Remark 6. The unicity of the decomposition in Theorem 1 may be shown as follows: say $R = R_1 \times R_2$ with R_1 unital and R_2 nilpotent. By the above remark we have $R_1 \subseteq \bar{R}$. On the other hand $\bar{e}_R = (\bar{e}_{R_1}, \bar{e}_{R_2}) = (\bar{e}_{R_1}, 0) = 1_{R_1}$, because R_1 is unital and R_2 is nilpotent. Since $R_1 = R \cdot R_1$, $R_1 \supseteq R \cdot \bar{e} = \bar{R}$, hence $R_1 = \bar{R}$. Notice that $R_2 = \{x \in R \mid x \cdot 1_{R_1} = 0\}$ thus $R_2 = N_R$.

The following theorem describes ring homomorphisms from a general ring to a finite field. It will be used in an essential way to reduce the key-recovery attack for ring homomorphic encryption schemes over reduced rings to the representation problem in black-box finite fields.

Theorem 3. *Let R, S be finite commutative rings with unity. Suppose that S is a local ring, and consider a nontrivial ring homomorphism $\varphi : R \to S$. Then, there exists a unique primitive idempotent e such that φ factors through its local component, i.e. φ is the composition $R \to Re \to S$.*

Proof. The homomorphism φ induces the homomorphism of rings $E(R) \to E(S) \simeq \mathbb{F}_2$, which is defined by a projection as in Proposition 1. In other words, there exists a unique $e \in R$ such that $\varphi(e) \neq 0$. Of course, $\varphi(e) = 1$. Using the explicit decomposition Theorem 2, we conclude that, indeed, φ factors through the projection $R \to R \cdot e$.

We have the following immediate consequence of the last theorem:

Corollary 1. *Let R be a finite (non-unital) commutative ring, and let k be a finite field. Then, there exists a unique primitive idempotent e such that φ factors through its local component, i.e. φ is the composition $R \to Re \to k$.*

Proof. It is enough to prove that $N_R \subseteq \ker(\varphi)$, which is obvious.

The following result is known to the specialists and establishes the existence of Teichmüler liftings. We express it in a very explicit way that shall be used in our applications:

Theorem 4. *Let R be a finite local ring with maximal ideal $\mathfrak{m}$ and residue field K of size q. Then for each $\bar{x} \in K$ there exists a unique $x \in R$ such that $x^q = x$ and $x \bmod \mathfrak{m} = \bar{x}$. Moreover, if $y \in R$ such that $y \bmod \mathfrak{m} = \bar{x}$, then $y^{q^n} = x$ for any n such that $\mathfrak{m}^n = 0$.*

Proof. Since R is complete in the $\mathfrak{m}-$adic topology, the first part of the theorem is just an application of Hensel's lemma. Let $y_i := y^{q^i}$, $\forall i \geq 1$, then we have $y_1 \equiv y \mod \mathfrak{m}$, so that $y_1 = y + m_1$, where $m_1 \in \mathfrak{m}$. Then $y_2 = (y + m_1)^q \equiv y^q \mod \mathfrak{m}^2$, therefore $y_2 = y_1 + m_2$ with $m_2 \in \mathfrak{m}^2$. By induction, $y_i = y_{i-1} + m_i$ with $m_i \in \mathfrak{m}^i$, hence $y_n = y_{n-1}$ for any n such that $\mathfrak{m}^n = 0$. Denoting by x this stationary value, we get that $x^q = x$ and $x \equiv y \mod \mathfrak{m}$.

Remark 7. Under the conditions of theorem 4, we have: $e(y) = y^{q^n(q-1)} \in \{0, 1\}$.

We have the following useful consequence of Theorem 4 :

Corollary 2. *Let $(R, \mathfrak{m})$ be a local ring and let $\pi : R \to R/\mathfrak{m}$ be the projection map. Then there exists a subset $X \subseteq R$ such that $(X, \oplus, \cdot)$ is isomorphic to the residue field $R/\mathfrak{m}$, where $x \oplus y = (x + y)^{q^n}$, and $\cdot$ is the usual multiplication on R (here q is the size of the residue field $R/\mathfrak{m}$, and n is the nilpotency index of the maximal ideal).*

Proof. Let X be the set of all $x \in R$ such that $x^q = x$, then one can verify that the map π induces an isomorphism of fields from X to the residue field of R.

Definition 6. *Let R be a finite commutative ring with unity. For a prime p, we denote by R_p the product of the local Artinian rings R_i, that occur in the decomposition of R, whose residue fields are of characteristic p. Moreover, for a prime p and a positive integer k, we denote by $R_{p,k}$ the product of the local Artinian rings R_i having residue fields isomorphic to $\mathbb{F}_{p^k}$. When $R = R_p$, we say that R is a p-power ring.*

Corollary 3. *Let R be a p-power ring whose Artinian local rings have residue fields isomorphic to a fixed finite field $\mathbb{F}_q$. Then there exists $S \subseteq R$, such that $(S, \oplus, \cdot) \simeq \prod_i R_i/\mathfrak{m}_i$, where $x \oplus y = (x+y)^{q^n}$, and $\cdot$ is the usual multiplication on R (here n is the nilpotency index of the ideal $\prod_i \mathfrak{m}_i$).*

The arguments of Corollary 2 can be extended immediately to this more general situation.

Remark 8. Notice that if $R = R_1 \times ... \times R_n$ is a finite ring, then R^{red}, the quotient of R by its nilradical, is isomorphic to $\prod_i R_i/\mathfrak{m}_i$. Therefore, the ring S in the last corollary is isomorphic to R^{red}. If R is a p-power ring then each $R_{p,k}$ satisfies the conditions of the last corollary. In particular, if R is also a BBR then each $R_{p,k}$ is a BBR, and then $R^{\text{red}}_{p,k}$ is a BBR for each k. Indeed, since S above is a subset of R, it inherits a BBR structure from R.

4 Computing the map e

In this section we investigate the complexity of the algorithm that computes the map $R \to E(R)$. The algorithm we present here was described in [11](see also [12], [5]), and is an adaptation of Shor's algorithm(see [32]).

Proposition 2. *Given a black-box semigroup G and an element $g \in G$, there is an efficient polynomial time quantum algorithm that computes $e(g)$. In particular, there is a quantum algorithm that computes the map $R \to E(R)$, where R is a finite commutative BBR.*

Interestingly enough, when R is a p-power BBR we can do much better. We have the following:

Proposition 3. *For any p-power black box ring R, there exist a classical polynomial time algorithm that computes the map $e : R \to E(R)$.*

Proof. Let $R = R_1 \times ... \times R_n$, where each R_i is a local finite ring with maximal ideal $\mathfrak{m}_i$, and residue field $R_i/\mathfrak{m}_i \simeq \mathbb{F}_{p^{k_i}}$. We may suppose that $\mathfrak{m}_i^{N_i} = (0)$, and that N_i is the least positive integer with this property. If $y = (y_1, ..., y_n)$, then by the remark above we obtain that

$$\begin{aligned} e(y) &= (e(y_1), ..., e(y_n)) = (y_1^{p^{k_1 N_1}(p^{k_1}-1)}, ..., y_n^{p^{k_n N_n}(p^{k_n}-1)}) \\ &= y^{p^{\max_i\{k_i N_i\}}(p-1)(p^2-1)...(p^{\max_i\{k_i\}}-1)}. \end{aligned}$$

Since $R_i \supset \mathfrak{m}_i \supset \mathfrak{m}_i^2 \supset ... \supset \mathfrak{m}_i^{n_i} = (0)$ and each $\mathfrak{m}_i^j/\mathfrak{m}_i^{j+1}$ is a $\mathbb{F}_{p^{k_i}}$-vector space, we get $|\mathfrak{m}_i^j/\mathfrak{m}_i^{j+1}| \geq p^{k_i}$ so that

$$|R_i| = \prod_{j=0}^{n_i-1} |\mathfrak{m}_i^j/\mathfrak{m}_i^{j+1}| \geq p^{k_i n_i}$$

Consequently, $p^{k_i n_i} \leq |R_i| \leq |R|$ and $k_i \leq \log_p |R|$ so that

$$e(y) = y^{p^{\lfloor \log_p |R| \rfloor}(p-1)(p^2-1)\dots(p^{\lfloor \log_p |R| \rfloor}-1)}$$

We can efficiently evaluate $e(y)$ by using the square-and-multiply techniques. More precisely, we need $\mathcal{O}(\log^2 |R|)$ multiplications to compute $z \mapsto z^{p^{\lfloor \log_p |R| \rfloor}}$ and also to compute $z \mapsto z^{p^i-1}$ for each $i \leq \lfloor \log_p |R| \rfloor$, so that to compute $e(y)$ we need $\mathcal{O}(\log^4 |R|)$ multiplications.

5 Computing the primitive idempotents of a ring

The purpose of this section is to prove the following theorem:

Theorem 5. *Let R be a finite commutative black box ring. Given a finite set of generators of R, there exists a polynomial-time quantum algorithm that computes all its primitive idempotents. In other words, we show an explicit way of computing the decomposition $R = \prod_i Re_i \times N_R$, where e_i are the primitive idempotents of R. Moreover, for each local Artinian component $R_i = Re_i$, there exists a subset R_i^{red} of R_i which, under the usual multiplication and a modified (explicitly classically computable) addition, becomes isomorphic to the residual field $R_i/\mathfrak{m}_i$ of R_i.*

The last part of the theorem says that there exists an explicit way of representing the reduced ring $R^{red} \simeq \prod_i R_i/\mathfrak{m}_i$ as a black-box ring (a similar situation as in the case of R_p and $R_{p,k}$, cf. 8).

Remark 9. As mentioned before, we shall use quantum computing only to determine each e_p (with p prime) and N_R, after that our algorithm will use only classical computing.

5.1 Computing the unital part

Let R be a non-unital commutative BBR. In this section we show how to compute the unit of its unital part $\bar{R}$. Fix a set of generators $G = \{g_1, ..., g_d\}$ of R. Let $\{e_1, \dots e_n\}$ be the set of primitive idempotents of R. If e and e' are idempotents in R we define the operation $e \vee e' = e \oplus e' \oplus ee'$, which is commutative and associative. Notice that if the primitive idempotent e_i occurs in the sum decomposition of at least one of the idempotents e and e', then e_i also occurs in the decomposition of $e \vee e'$.

Theorem 6. *Let $G = \{g_1, \ldots, g_d\}$ be the generating set of a non-unital ring R. Then*

$$\bar{e} = \bigvee_{j=1}^{d} e(g_j)$$

is the unit of its unital part $\bar{R}$.

Proof. For every $k \in \overline{1,n}$, let $R_k = Re_k$ and let $\mathfrak{m}_k$ be its maximal ideal. It is enough to show that there exists at least one $i \in \overline{1,d}$ such that $g_i \cdot e_k \notin \mathfrak{m}_k$. Assume by contradiction that $g_i \cdot e_k \in \mathfrak{m}_k$ for all $i \in \overline{1,d}$. Then the whole generating set G sits inside de kernel of the following composition of homomorphisms:

$$R \to \bar{R} \to \bar{R}/Nil(\bar{R}) \simeq \prod_{k=1}^{n} R_k/\mathfrak{m}_k,$$

and this is impossible.

When R is a non-unital commutative BBR, we compute first each $e(g_i)$ using the modified Shor's Algorithm presented in Section 4, and then $\bar{e}$. Notice that the set $G\bar{e} := \{g_1\bar{e}, \ldots, g_d\bar{e}\} \subseteq \bar{R}$ is a system of generators of $\bar{R}$, so that from now on we shall work only on $\bar{R}$, equivalently we may suppose that R is a unital commutative BBR.

5.2 Computing the $p-$power parts of a unital ring

The purpose of this subsection is to show how to decompose a unital commutative ring into his $p-$power parts, where p is a positive prime integer. We don't need a system of generators for this decomposition.

Theorem 7. *Let R be a unital finite commutative BBR. There exists a polynomial time quantum algorithm that determines for all primes p an idempotent e_p, such that $R = \prod_p Re_p$, and Re_p is a p-power BBR.*

Proof. Since R is finite, only finitely many e_p will be nonzero and we shall describe them shortly. Moreover, for every p, $R_p := Re_p$ is a semi local ring with all its residual characteristics equal to p. We describe now the algorithm:

1. Use Shor's quantum algorithm to compute the characteristic of R, i.e. the minimal positive integer N such that $N \cdot 1_R = 0$ (see section 4).
2. Use Shor's quantum factorization algorithm to compute the prime factorization of $N = \prod_p p^{\alpha_p}$ (see [32]).
3. Use Euclidean algorithm to compute integers u_p such that $\frac{N}{p^{\alpha_p}} \mid u_p$ and $\sum_p u_p = 1$.
4. Set $e_p := u_p \cdot 1_R$.

It is easy to check that, indeed, e_p are orthogonal idempotents with sum 1_R. Moreover, the ring R_p has all its residual characteristics equal to p. Exactly as at the end of the previous, it can be shown that R_p inherits a BBR structure from R.

5.3 Computing $R_{p,k}$'s

The aim of this subsection is to show how to compute the idempotents $e_{p.k}$, which determine the rings $R_{p,k}$. As explained in Remark 9, from now on all algorithms proposed are classical. We have the following result:

Theorem 8. *Let R be a p-power BBR, and let $G = \{g_1, \dots, g_d\} \subseteq R$ be a set of generators for the ring R. There exists an explicit polynomial time algorithm that determines for all positive integers k an idempotent $e_{p,k}$ such that $R = \prod_k Re_{p,k}$ and $R_{p,k} = Re_{p,k}$ is a p-power BBR with all its residue fields isomorphic to $\mathbb{F}_{p^k}$.*

Proof. Let $\{e_1, \dots e_n\}$ be the set of primitive idempotents of R. We shall construct the $e_{p,k}$'s inductively:

Algorithm 1 Compute $e_{p,k}$

```
$\bar{e}_{p,0} := 1_R$
$k = 0$
while $\bar{e}_{p,k} \neq 0$
$k = k + 1$
        for $i = 1$ to $d$ do
            $\mathfrak{e}_{i,k} := e(g_i \cdot \bar{e}_{p,k-1} - g_i^{p^k} \cdot \bar{e}_{p,k-1})$
        end for
$\bar{e}_{p,k} = \bigvee_{i=1}^{d} \mathfrak{e}_{i,k}$
$e_{p,k} = \bar{e}_{p,k-1} - \bar{e}_{p,k}$
end while
return $e_{p,k}, k \geq 1$
```

We prove by induction on k that all residue fields of the local Artinian components of $Re_{p,k}$ are isomorphic to $\mathbb{F}_{p^k}$. Consider a primitive idempotent e_j. If $e(g_i - g_i^p) \cdot e_j = e_j$ for some i, then $R_j/\mathfrak{m}_j \not\simeq \mathbb{F}_p$. Indeed, otherwise $g_i e_j \equiv (g_i e_j)^p = g_i^p e_j \mod \mathfrak{m}_j$, so that

$$0 = e(g_i e_j - g_i^p e_j) = e(g_i - g_i^p) e_j = e_j,$$

which is a contradiction. Hence $\bar{e}_{p,1}$ is a sum of primitive idempotents with corresponding residue fields non-isomorphic to $\mathbb{F}_p$. Moreover, $\bar{e}_{p,1}$ is the sum of all primitive idempotents with corresponding residue fields non-isomorphic to $\mathbb{F}_p$. Let e_j be a primitive idempotent with corresponding residue field non-isomorphic to $\mathbb{F}_p$. Since $R_j/\mathfrak{m}_j$ is non-isomorphic to $\mathbb{F}_p$ and $\{g_1 e_j \mod \mathfrak{m}_j, ..., g_d e_j \mod \mathfrak{m}_j\}$ generates $R_j/\mathfrak{m}_j$, there exist an i such that $g_i e_j - (g_i e_j)^p \not\in \mathfrak{m}_j$, therefore $e(g_i - g_i^p) e_j = e_j$, which proves our claim. In particular, $e_{p,1}$ is the sum of all primitive idempotents with corresponding residue fields isomorphic to $\mathbb{F}_p$. The same argument works inductively for any k, because multiplication by $\bar{e}_{p,k-1}$ restricts to the Artinian local components of R with corresponding residue fields of size at least p^k.

5.4 Computing the Artinian local components of $R_{p,k}$

The purpose of this section is to show how to compute the primitive idempotents of a ring R with isomorphic residue fields $\mathbb{F}_q = \mathbb{F}_{p^k}$. The first observation is that we can work with R^{red}, instead of R. Indeed, as explained in Remark 8, R^{red} has a well defined BBR structure, and in this case it is isomorphic to a product of fields, each being isomorphic to $\mathbb{F}_q$. Moreover, since R^{red} is just a subset of R and the multiplication of R^{red} is inherited from R, the primitive idempotents of R are the same as the primitive idempotents of R^{red}.

Computing the primitive idempotents when $k = 1$. We are in the case $R = \prod_i Re_i$ with $Re_i \simeq \mathbb{F}_p, \forall i$. Let $G = \{g_1, \ldots, g_d\}$ be a generating set of R. We distinguish two cases:

• The case $p = 2$. In this case, R is an idempotent ring of characteristic 2, i.e. $R \simeq \mathbb{F}_2^n$. The following algorithm computes the primitive idempotents of $R_{2,1}$. We shall use the following notation for X a subset of a ring R, and $r \in R$ an element of the ring:

$$rX := \{rx | x \in R\}.$$

Algorithm 2 Compute the primitive idempotents of $R_{2,1}$

```
$X_0 := \{0, 1\}$
for $i = 1$ to $d$ do
    $X_i := g_i X_{i-1} \bigcup (1 - g_i) X_{i-1}$
end for
return $X_d \setminus \{0\}$
```

Notice that for each i, X_i consists of elements which are mutual orthogonal, so that it has no more than $n+1$ elements, i.e. at most a polynomial (in the security parameter) number of elements. Moreover, we claim than $X_n \setminus \{0\} := \{f_1, \ldots f_r\}$ is the set of all primitive idempotents of R. Notice that each f_j is a product of elements of R, each factor being equal to either g_i or $1 - g_i$, for some i. This means that either $g_i f_j = 0$ or $(1-g_i) f_j = 0 \Leftrightarrow g_i f_j = f_j$, for all $i \in \overline{1, n}$, therefore G generates only $\mathbb{F}_2 \cdot f_j$ inside Rf_j, which is possible only if f_j is primitive.

• The case $p \geq 3$, $R \simeq \mathbb{F}_p^n$. Consider the following algorithm, where $x \in R$, $r \in \{0, 1, ..., p-1\}$:

Algorithm 3 $\mathcal{A}(\mathbf{x}, \mathbf{r})$

```
Compute $x^{\pm}(r) := \frac{(x-r)^{p-1} \pm (x-r)^{\frac{p-1}{2}}}{2}$
return: $\{x^+(r), x^-(r)\} \setminus \{0\}$
```

Notice that if $a \in \mathbb{F}_p$, then $\chi(a) := a^{\frac{p-1}{2}}$ is the Legendre symbol, i.e. the primitive quadratic character on $\mathbb{F}_p$, and $e(a) = a^{p-1}$. Let $x = \sum_i x_i e_i \in R$, with $x_i \in \mathbb{F}_p$, then $x^{\pm}(r) \cdot e_i = \frac{\chi(x_i - r) \pm \chi(x_i - r)^2}{2} \cdot e_i$. The algorithm $\mathcal{A}(\mathbf{x}, \mathbf{r})$ returns $\emptyset$ or $\{1\}$ if and only if either $x_i = r$, $\forall i$ or $\chi(x_i - r)$ is constant for all i. We have the following:

Proposition 4. *Let $x \in R$ be such that $x \neq a \cdot 1_R$ for some $a \in \mathbb{F}_p$. Then, the probability that the algorithm $\mathcal{A}(\mathbf{x}, \mathbf{r})$ returns a set of two different values is at least $\frac{1}{2} - \frac{1}{2p} \geq \frac{1}{3}$, when r is uniformly chosen from the set $\{0, 1, ..., p-1\}$.*

Proof. It is enough to compute the probability for $n = 2$, i.e. $x = (a, b)$ with $a \neq b \in \mathbb{F}_p^{\times}$. The experiment is successful if $\chi((a-r)(b-r)) = -1$. To count how many r's have this property, we count first how many r's satisfy $\chi((a-r)(b-r)) = 1$, but this is equivalent to finding the number of solutions of the equation $y^2 = (x-a)(x-b)$ over $\mathbb{F}_p$ with $y \neq 0$, which is given by

$$\begin{aligned}
\sum_{x \neq a,b} \frac{1 + \chi((x-a)(x-b))}{2} &= \frac{p-2}{2} + \frac{1}{2} \sum_{x \neq a,b} \chi((x-a)(x-b)) \\
&= \frac{p-2}{2} + \frac{1}{2} \sum_{x \neq a,b} \chi\left(\frac{x-a}{x-b}\right) \\
&= \frac{p-2}{2} + \frac{1}{2} \sum_{x \neq 0,1} \chi(x) = \frac{p-3}{2},
\end{aligned}$$

where the second to the last equality follows from the fact that the map $x \mapsto \frac{x-a}{x-b}$ is a bijection from $\mathbb{F}_p \setminus \{a, b\}$ to $\mathbb{F}_p \setminus \{0, 1\}$, and the last equality is a consequence of $\sum_{x \in \mathbb{F}_p^{\times}} \chi(x) = 0$, for any nontrivial character. Thus, the probability of success is greater than or equal to $\frac{p-1}{2p}$, which is exactly our claim.

We use $\mathcal{A}(\mathbf{x}, \mathbf{r})$ in the following important algorithm:

Algorithm 4 $\mathfrak{Equal}(x)$

```
$X_0 := \{0, 1\}$
    for $i = 1$ to $\Theta(\lambda)$ do
        Pick $r$ uniformly random from $\{0, 1, ..., p-1\}$, run $\mathcal{A}(\mathbf{x}, \mathbf{r})$
        If $\mathcal{A}(\mathbf{x}, \mathbf{r})$ returns $\emptyset$, then return: $F := \{1\}$
        else $X_i := \bigcup_{y \in \mathcal{A}(\mathbf{x}, \mathbf{r})} y X_{i-1}$
    end for
return: $F := X_{\Theta(\lambda)} \setminus \{0\}$
```

Proposition 5. *Let $x \in R \setminus \{0\}$. Then, the algorithm $\mathfrak{Equal}(x)$ returns a set of orthogonal idempotents F such that $x = \sum_{f \in F} x_f \cdot f$, $x_f \in \mathbb{F}_p^\times$ with probability greater than $1 - (\frac{2}{3})^{\Theta(\lambda)}$.*

Proof. It is easy to see that $e(x) = \sum_{f \in F} f$, and $xf \in \mathbb{F}_p^\times f$, $\forall f \in F$, then:

$$x = x \cdot e(x) = \sum_{f \in F} xf,$$

which proves the required equality. The estimated probability follows from Proposition 4.

Now, we are proceeding similarly to the case $p = 2$ to compute the primitive idempotents of $R_{p,1}$:

Algorithm 5 Compute the primitive idempotents of $R_{p,1}$

```
$X_0 := \{0, 1\}$
    for $i = 1$ to $d$ do
        Run $\mathfrak{Equal}(g_i)$, and let $F(g_i)$ be the output
        $X_i := F(g_i)X_{i-1} \cup (1 - e(g_i))X_{i-1}$
    end for
return: $X_d \setminus \{0\}$
```

where for two subsets $X, Y \subseteq R$, $X \cdot Y := \{x \cdot y | x \in X, y \in Y\}$.

The above algorithm returns with overwhelming probability a set of orthogonal idempotents F for which $g_i \cdot f = a(g_i, f) \cdot f$ for some $a(g_i, f) \in \mathbb{F}_p$, $\forall i \in \overline{1, d}$, i.e. all the components of g_i corresponding to the primitive idempotents in f are equal. Consequently, since $\{g_1, ..., g_d\}$ is a set of generators of R, with overwhelming probability, all primitive idempotents of R will appear in $X_d \setminus \{0\}$.

Computing the primitive idempotents when $k \geq 2$. In this section, we assume that $R = \prod Re_i$, where for all $i \in \overline{1, n}$, $Re_i \simeq \mathbb{F}_q = \mathbb{F}_{p^k}$ with $k \geq 2$. We shall denote by $\pi_i : R \to \mathbb{F}_q$, $\forall i$ the projection onto the i^{th}- component. If $x \in R$, then computing x^p has the effect of acting with the Frobenius automorphism of $\mathbb{F}_q$ on each primitive component. Moreover, if s_j represents the $j^{th}-$ elementary symmetric polynomial in k variables, then computing $s_j(x, x^p, \dots x^{p^{k-1}})$ will produce on each primitive component the coefficient of X^{k-j} of the characteristic polynomial $P(X)$ of that component. It is well known that, since the characteristic polynomial of some number of $\mathbb{F}_q$ is just a power of its minimal polynomial, we get that two numbers in $\mathbb{F}_q$ have the same characteristic polynomial if and only if they are Galois conjugates. Notice also that for any $x \in R$ and every $j \in \overline{1, k}$:

$$s_j(x, x^p, \dots, x^{p^{k-1}}) \in \prod_i F_p e_i.$$

The following algorithm takes as input a non-zero element x and outputs a set of orthogonal idempotents, such that on each one of them, the corresponding primitive components are Galois conjugates.

Algorithm 6 $\mathfrak{Conj}(x)$

```
$F := \{0,1\}$
    **for** $i = 1$ to $k$
        Compute $u_j(x) := s_j(x, x^p, \dots x^{p^{k-1}})$
        $E_j := \mathfrak{Equal}(u_j(x))$
        $F = E_j \cdot F \bigcup (1 - e(u_j(x))) \cdot F$
    **end for**
**return:** $F \setminus \{0\}$
```

Now we collect all the idempotents returned by applying $\mathfrak{Conj}$ to the generating set:

Algorithm 7 $\mathfrak{Conj}G$

```
$F := \{0,1\}$
    **for** $i = 1$ to $d$
        $X_i := \mathfrak{Conj}(g_i)$
        $F = E_i \cdot F \bigcup (1 - e(g_i)) \cdot F$
    **end for**
**return:** $F \setminus \{0\}$
```

The above algorithm allows us to reduce to the case in which the primitive components of any element of the generating set are Galois conjugates, namely for each $f \in \mathfrak{Conj}G$, replace R by Rf, and G by fG.

Lemma 1. *All primitive components of $x \in R$ are Galois conjugates if and only if $\mathbb{F}_p[x]$ is a field.*

Proof. Observe that the restriction $\pi_1 : \mathbb{F}_p[x] \to \mathbb{F}_q$ is injective when all primitive components of $x \in R$ are Galois conjugates, so that $\mathbb{F}_p[x]$ is a field. Conversely, let x_i and x_j be two distinct primitive components of $x \in R$, and let $Q(X)$ be the minimal polynomial of x_i over $\mathbb{F}_p$. We get that the i^{th} and j^{th} components of $Q(x) \in R$ are 0 and $Q(x_j)$, respectively. If $Q(x_j) \neq 0$, then $Q(x)$ were a zero divisor in R, so that it couldn't be invertible in R, consequently also not in $\mathbb{F}_p[x]$. So $Q(x_j) = 0$, which proves that x_i and x_j are Galois conjugate.

Let $\mathrm{GalConj}(R)$ be the set of all $x \in R$ satisfying Lemma 1, then for any $x \in \mathrm{GalConj}(R)$ we define the size:

$$k(x) = [\mathbb{F}_p[x] : \mathbb{F}_p] = [\mathbb{F}_p[\pi_i(x)] : \mathbb{F}_p], \forall i.$$

It is clear that $k(x) = \min\{j \in \mathbb{N} | x^{p^j} = x\}$, and if R is a BBR then $k(x)$ is polynomial in the security parameter λ.

Lemma 2. *Let $x, y \in$ GalConj(R) with $\gcd(k(x), k(y)) = 1$, then $\mathbb{F}_p[x, y]$ is a field.*

Proof. Let $i \in \{2, ..., n\}$, then $x_i = x_1^{p^{u_i}}$, and $y_i = y_1^{p^{v_i}}$, for some integers u_i, v_i. Since $(k(x), k(y)) = 1$, by the Chinese Remainder Theorem, there exist an integer N_i such that $N_i \equiv u_i \pmod{k(x)}$, and $N_i \equiv v_i \pmod{k(y)}$, so that $x_i = x_1^{p^{N_i}}$, and $y_i = y_1^{p^{N_i}}$. Consequently, the restriction of π_1, $\pi_1 : \mathbb{F}_p[x, y] \to \mathbb{F}_q$ is injective, hence $\mathbb{F}_p[x, y]$ is a field.

Remark 10. A useful consequence of the last lemma is that if $x, y \in \mathrm{GalConj}(R)$, then any polynomial with integer coefficients in x and y is also in $\mathrm{GalConj}(R)$.

The rest of this section is heavily influenced by the results of [25], where R is just a finite field. The main arguments are there, we just verified that they can be extended to our case. First of all we show that there exist $\bar{g} \in \mathrm{GalConj}(R)$ with $k(\bar{g}) = k$. The following algorithm is called **combine_gen**, we shall make it suitable to our situation:

Algorithm 8: combine_gen(a, b)

```
0: Let $a, b \in \mathrm{GalConj}(R)$
1: Find $k_a | k(a)$ and $k_b | k(b)$ such that:
       $\gcd(k_a, k_b) = 1, \mathrm{lcm}(k_a, k_b) = \mathrm{lcm}(k(a), k(b))$
2: Find $a' \in \mathbb{F}_p[a], b' \in \mathbb{F}_p[b]$ such that $k(a') = k_a$, $k(b') = k_b$.
3: return: $a' + b'$
```

Step 1 and Step 2 are explained in [25], and the arguments also work in our case because $\mathbb{F}_p[a], \mathbb{F}_p[b]$ are fields. Since $\gcd(k_a, k_b) = 1$, by Lemma 2, $\mathbb{F}_p[a, b]$ is a field. Obviously $\mathbb{F}_p[a, a + b] = \mathbb{F}_p[a + b, b] = \mathbb{F}_p[a, b]$ so that

$$\mathrm{lcm}(k(a'), k(a' + b')) = \mathrm{lcm}(k(a' + b'), k(b')) = \mathrm{lcm}(k(a'), k(b')) = k(a') \cdot k(b').$$

We get that $k(a' + b') = k(a') \cdot k(b') = \mathrm{lcm}(k(a), k(b))$, also by the last remark we obtain $a' + b' \in \mathrm{GalConj}(R)$.

Algorithm 9: Computing $\bar{g}$

```
0: Let $\{g_1, ..., g_d\}$ be a generating set for $R$.
1: Set $\bar{g} := g_1$
2:      for $i = 2$ to $d$ do
```

```
        $\bar{g} :=$ **combine_gen**$(\bar{g}, g_i)$
    **end for**
**return:** $\bar{g}$
```

It is clear that $k(\bar{g}) = \mathrm{lcm}(k(g_1), ..., k(g_d))$, and $\bar{g} \in \mathrm{GalConj}(R)$. Since $\mathbb{F}_q$ is generated as a ring by $\{\pi_1(g_1), ..., \pi_1(g_d)\}$, $\mathrm{lcm}(k(g_1), ..., k(g_d)) = k$. In other words $k(\bar{g}) = k$, i.e. $\mathbb{F}_p[\bar{g}] \simeq \mathbb{F}_q$.

By the well-known dual basis theorem [24], there exist an $\mathbb{F}_p$-basis $h_1, ..., h_k$ of $\mathbb{F}_p[\bar{g}]$ such that $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\bar{g}^i h_j) = \delta_{i+1,j}$, where $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) := x + x^p + ... + x^{p^{k-1}}$, for any $x \in R$.

Algorithm 10 Compute the primitive idempotents of $R_{p,k}$

```
    **for** $i = 1$ to $d$ **do**
        Compute $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j)$, $\forall j$
        Let $X_i := \bigcup_j \mathfrak{Equal}(\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j))$
    **end for**
Let $Y := \cup_i X_i = \{y_1, ..., y_\ell\}$
Let $F := \{0, 1\}$
    **for** $i = 1$ to $\ell$ **do**
        $F := y_i F \cup (1 - y_i) F$
    **end for**
**return:** $\bar{F} := F \setminus \{0\}$
```

To prove that $\bar{F}$ consists of all primitive idempotents of R, notice first that $\sum_{f \in \bar{F}}^{\oplus} f = 1$. Also, it is easy to see that

$$f \in \bar{F} \Leftrightarrow \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j) f \in \mathbb{F}_p f, \forall i, j.$$

Let $x_i := g_i - \sum_{j=1}^{k} \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j) \cdot \bar{g}^{j-1}, \forall i \in \overline{1, d}$.

$$\begin{aligned}
\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_i h_j f) &= \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j f) - \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\sum_{\ell=1}^{k} \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_\ell) f \bar{g}^{\ell-1} h_j) \\
&= \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j) f - \sum_{j=1}^{k} \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_\ell) f \cdot \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\bar{g}^{\ell-1} h_j) \\
&= \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j) f - \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j) f = 0
\end{aligned}$$

We obtained $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_i h_j f) = \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_i h_j) f = 0$, $\forall j \in \overline{1, d}, f \in \bar{F}$. Since $\sum_{f \in \bar{F}}^{\oplus} f = 1$, each primitive idempotent e occurs in the decomposition of at least one f, so that $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_i h_j)e = \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_i h_j e) = 0$, for all primitive idempotents e. Notice that $\{h_j e | j \in \overline{1,d}\}$ is the dual basis of $\{\bar{g}^{j-1}e | j \in \overline{1,d}\}$, for every primitive idempotent e, which yields $x_i e = 0$, $\forall e$, hence $x_i = 0$. We have:

$$g_i f = \sum_{j=1}^{k} \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j) f \cdot \bar{g}^{j-1} \in \mathbb{F}_p[\bar{g}], \forall i \in \overline{1,d},$$

in other words, the ring generated by $\{g_i f | i \in \overline{1,d}\}$ is a subring of the field $\mathbb{F}_p[\bar{g}]$, so that it has no zero divisors. On the other hand, $\{g_i f | i \in \overline{1,d}\}$ generates Rf, consequently Rf has no zero divisors, hence each $f \in \bar{F}$ is a primitive idempotent. Since $\sum_{f \in \bar{F}} f = 1$, $\bar{F}$ contains all primitive idempotents of R, and we are done.

6 Decrypting in Ring Homomorphic Encryption Schemes

6.1 IND-CCA^1−attack on ring homomorphic encryption schemes over general quasi-unital rings

We present in this section one of our cryptanalysis results:

Theorem 9. *If the ciphertext space of a ring homomorphic encryption scheme is a quasi-unital ring, then the scheme is not IND-CCA^1−secure.*

Proof. Suppose that R and S are the ciphertext space, and respectively the plaintext space of a ring homomorphic encryption schemes, and that S is a quasi-unital ring. We use all the results in Section 5 to find the primitive idempotents of R. Then we start decrypting the primitive idempotents, using the decryption oracle, until we find a nonzero decryption, say $f \overset{\mathrm{Dec}}{\longmapsto} m$, where Rf has residual characteristic equal to p. Then we use m and 0 in S in the IND-CCA^1 experiment. Fix a positive integer $n > \log_p |R|$, and let $t = p^n(p-1) \cdot \ldots \cdot (p^n - 1)$. Since any ciphertext $c \in Enc(m)$ satisfies $e(cf) = (cf)^t = f$, and any $c \in Enc(0)$ satisfies $e(cf) = (cf)^t = 0$ (cf. Proposition 3), the strategy for the decryption of c is clear, and is pictured in the following commutative diagram:

$$\begin{tikzcd} R \arrow[r, "\cdot\bar{e}"] \arrow[d, "\mathrm{Dec}"'] & \bar{R} \arrow[r, "f\cdot"] \arrow[d, "\mathrm{Dec}"'] & Rf \arrow[d, "\mathrm{D}"] \\ S \arrow[r, "="] & S \arrow[r, "\cdot m"] & Sm \end{tikzcd}$$

Remark 11. As we mentioned in the Introduction, we have used quantum computations only in the process of finding the primitive idempotents of the ciphertext space. After the ciphertexts are sent to the challenger, only classical algorithms are used to win the game. Thus, we have constructed a quantum-classical IND-CCA^1 attack. Please also notice that we have used the assumption that the plaintext is quasi-unital because otherwise, all the primitive idempotents of R decrypt to 0. On the other hand, if S is quasi-unital, then S^{red} is non-trivial, i.e. it has at least one non-trivial primitive idempotent. Finally, since Dec is a non-trivial homomorphism of rings we can find f and m as above.

6.2 Reduced black-box rings of small prime characteristic

In this section, we extend the results of [25] to the case of a reduced p-power BBR, equivalently a finite product of finite fields, all of characteristic p. As in [25], we have the following:

Definition 7. *(Representation Problem) Let R be a reduced p-power BBR, and let $G = \{g_1, ..., g_d\}$ be a generating set for R. If $x \in R$, then finding a multivariate polynomial $P(X_1, ..., X_d) \in \mathbb{F}_p[X_1, ..., X_d]$ such that $x = P(g_1, ..., g_d)$ is called the representation problem.*

We state the following extension of Theorem 1 from [25]:

Theorem 10. *The representation problem for a reduced p-power BBR is efficiently reducible to the representation problem for $\mathbb{F}_p$.*

Proof. The results of sections 5.3 and 5.4 show how to compute the primitive idempotents of the reduced p-power BBR in terms of the generating set, more precisely as multi-variate polynomials in the elements of the generating set. Hence, we reduce the representation problem for a p-power BBR to the representation problem for each local Artin component of it, and since each local Artin component is a finite field of characteristic p, our result follows from Maurer and Raub's result.

Consequently, we have the following:

Corollary 4. *If R is a reduced p-power BBR and p is small, then the representation problem for R is efficiently solvable.*

Remark 12. We refer the reader to [25] for the connection between the representation problem and the extraction and isomorphism problems for black-box fields. As in [25], our result shows that the extraction and isomorphism problems for a reduced p-power BBR are efficiently reducible to the representation problem for $\mathbb{F}_p$.

6.3 Key-recovery attack on ring homomorphic encryption schemes over reduced rings of smooth characteristic

We investigate in this section the security of ring homomorphic encryption scheme with plaintext space a reduced ring of smooth characteristic. This means that the ciphertext space is a product of fields, such that each field that occurs in the product has small characteristic.

Theorem 11. *Let $(R, S, \mathrm{Dec}, \mathrm{Enc})$ be a ring homomorphic encryption scheme with plaintext space S, a reduced ring of smooth characteristic. Then there exist an efficient (quantum) key-recovery attack.*

Proof. We consider the following commutative diagram:

$$\begin{tikzcd}
R \arrow[r, "\cdot\bar{e}_R"] \arrow[d, "\mathrm{Dec}"'] & \bar{R} \arrow[r] \arrow[d, "\mathrm{Dec}"'] & \prod_p Re_p(R) \arrow[r] \arrow[d, "\mathrm{Dec}"'] & \prod_{p,k} Re_{p,k}(R) \arrow[r] \arrow[d, "\mathrm{Dec}"'] & Re_j \arrow[r] \arrow[d, "\mathrm{D_j}"] & (R_j^{red}, \oplus, \cdot) \arrow[dl, "\Psi_j"] \\
S \arrow[r, "="] & \bar{S} \arrow[r] & \prod_p Se_p(S) \arrow[r] & \prod_{p,k} Se_{p,k}(S) \arrow[r] & S\mathrm{Dec}(e_j) &
\end{tikzcd}$$

where $e_{p,k}(R)$, respectively $e_{p,k}(S)$, are the primitive idempotents corresponding to the decomposition in local fields with residue fields isomorphic to $\mathbb{F}_{p^k}$ in R, respectively in S. Moreover, R_j^{red} is the Teichmüller lifting of the residue field $R_j/\mathfrak{m}_j$ (cf. Corollary 3 and Remark 8). As we have seen before, each primitive idempotent of S corresponds to a unique primitive idempotent of R, which decrypts to it (cf. Corollary 1). Consider the following algorithm:

1. Compute the idempotent structure on R using the generating set G, that is compute all $e_j(R)$. For each e_j find $\mathrm{Dec}(e_j)$ using the decryption oracle; these are necessarily either primitive idempotents of S or equal to 0.
2. Record the triples $(e_j, \tilde{e}_j := \mathrm{Dec}(e_j), \mathrm{Size}(R_j^{red}))$ with $\tilde{e}_j \neq 0$. Set $\tilde{E} := \{e_j \mid \tilde{e}_j \neq 0\}$.
3. Let $c \in R$. Compute $\{c \cdot e_j \mid e_j \in \tilde{E}\}$, and $c_j := (c \cdot e_j)^{q^n}$ for large enough n.
4. Put $\mathrm{Dec}(c) = \sum_{e_j \in \tilde{E}} \Psi_j(c_j)$.

We claim that $\Psi_j : R_j^{red} \to S\tilde{e}_j$ is an isomorphism for all j such that $e_j \in \tilde{E}$. It is clear that Ψ_j is injective. On the other hand, it is easy to see, using Enc and going backwards in the diagram from $S\tilde{e}_j$ to R_j^{red}, that is also surjective. Now, if a generator for $S \cdot \tilde{e}_j$ is given, then we can use *Enc* again, then pass through all the steps described above to find a generator in R_j^{red} that maps under Ψ_j to the given generator. Thus, we have a set of generators in R_j^{red} that is mapped to the given set of generators of $S \cdot \tilde{e}_j$. Now, the result of Maurer and Raub ([25], Theorem 1) shows that the map Ψ_j is efficiently computable, which ends the argument.

Remark 13. In general, if the characteristic of the plaintext space is any number, the above argument shows that decryption map may be computed correctly, when the representation problem is solvable for any prime divisor of it.

Remark 14. Since our strategy for the key-recovery attack uses in an essential way the computation of idempotents, we cannot deduce any information about the nilpotent part. This is why we have to assume in the theorem that the plaintext S is a reduced ring.

References

1. Armknecht, F.; Gagliardoni, T.; Katzenbeisser, S.; Peter, A.: *General Impossibility of Group Homomorphic Encryption in the Quantum World*, International Workshop on Public Key Cryptography - PKC 2014, Lecture Notes in Computer Science, vol. 8383, pp. 556 - 573.

2. Armknecht, F.; Katzenbeisser, S.; Peter, A.: *Group Homomorphic Encryption: Characterizations, Impossibility Results, and Applications* in Designs, Codes and Cryptography, Volume 67, Number 2, 2013, pp. 209–232.
3. Arvind, V.; Das, B.; Mukhopadhyay, P.: *The Complexity of Black-Box Ring Problems*, COCOON 2006: Computing and Combinatorics, Lecture Notes in Computer Science, vol. 4112, pp. 126 - 135.
4. Atiyah, M. F.; Macdonald, I. G.: *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.
5. Barcau, M.; Paşol, V.: *Ring Homomorphic Encryption Schemes*, available at https://eprint.iacr.org/2018/583.pdf.
6. Barcau, M.; Paşol, V.: *Bounded Fully Homomorphic Encryption from Monoid Algebras*, available at https://eprint.iacr.org/2018/584.pdf.
7. Brakerski, Z.; Vaikuntanathan, V.: *Efficient fully homomorphic encryption from (standard) LWE*, In IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, Rafail Ostrovsky editor, pp. 97 - 106.
8. Brakerski, Z.: *Fully homomorphic encryption without modulus switching from classical GapSVP*, In CRYPTO 2012, pp. 868 - 886.
9. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: *(Leveled) fully homomorphic encryption without bootstrapping*, Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, ITCS 2012, pp. 309 - 325.
10. Chenal, M.; Tang, Q.: *On Key Recovery Attacks Against Existing Somewhat Homomorphic Encryption Schemes*, International Conference on Cryptology and Information Security in Latin America, LATINCRYPT 2014, Lecture Notes in Computer Science, Vol. 8895, pp. 239 - 258.
11. Childs, A.M.; Ivanyos, G.: *Quantum computation of discrete logarithms in semigroups*, Journal of Mathematical Cryptology, Volume 8, Number 4, 2014, pp. 405-416.
12. Childs, A.M.; van Dam, W.: *Quantum algorithms for algebraic problems*, Reviews of Modern Physics 82, 2010, pp. 1 - 52.
13. Coron, J-S., Mandal, A., Naccache, D., Tibouchi, M.: *Fully homomorphic encryption over the integers with shorter public keys*, P. Rogaway editor, Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara 2011, Lecture Notes in Computer Science, vol. 6841, Springer, 2011, pp. 487 - 504.
14. van Dijk, M.; Gentry, C.; Halevi, S.; Vaikuntanathan, V.: *Fully homomorphic encryption over the integers*, In EUROCRYPT, 2010, pp. 24 - 43. Full Version in http://eprint.iacr.org/2009/616.pdf.
15. Doröz, Y.; Hoffstein, J.; Pipher, J.; Silverman, J.H.; Sunar, B.; Whyte, W.; Zhang, Z.: *Fully Homomorphic Encryption from the Finit Field Isomorphism Problem*, available https://eprint.iacr.org/2017/548.
16. Gentry, C.: *A fully homomorphic encryption scheme*, PhD thesis, Stanford University, 2009.
17. Gentry, C.: *Fully homomorphic encryption using ideal lattices*, In STOC 2009, Proceedings of the 41st annual ACM symposium on Theory of computing, pp. 169 - 178.
18. Gentry, C.: *Computing arbitrary functions of encrypted data*, Communications of the ACM, Vol. 53, Issue 3, March 2010, pp. 97 - 105.
19. Gentry, C., Halevi, S.: *Fully homomorphic encryption without squashing using depth-3 arithmetic circuits*, In IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, Rafail Ostrovsky editor, pp. 107 - 109.

20. Gentry, C., Sahai, A., Waters, B.: *Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based*, Advances in Cryptology - CRYPTO 2013, Lecture Notes in Computer Science, Vol. 8042, 2013, pp. 75 - 92.
21. Halevi, S.: *Homomorphic Encryption*, Chapter 5: Tutorials on the Foundations of Cryptography, part of the Information Security and Cryptography book series, Springer Verlag 2017, pp. 219 - 276.
22. Hardy, G.H.; Wright, E.M.: *An Introduction to the Theory of Numbers*, Oxford University Press, 5th edition.
23. Loftus, K.; May, A.; Smart, N.P.; Vercauteren, F.: *On CCA-Secure Somewhat Homomorphic Encryption*, Selected Areas in Cryptography, SAC 2011, Lecture Notes in Computer Science, Vol. 7118, pp. 55 - 72.
24. Lidl, R.; Niederreiter, H.: *Finite Fields*, Encyclopedia of Mathematics and its Applications, Vol. 20, Cambridge University Press, 2nd edition, 1997.
25. Maurer, U.; Raub, D.: *Black-Box Extension Fields and the Inexistence of Field-Homomorphic One-Way Permutations*, Advances in Cryptology - ASIACRYPT 2007, Lecture Notes in Computer Science, Vol. 4833, pp. 427 - 443.
26. McDonald, B.R.: *Finite Rings with Identity*, Pure and Applied Mathematics 28, Marcel Dekker Inc., New York, 1974.
27. Ostrovsky, R.; Skeith III, W.E.: *Communication Complexity in Algebraic Two-Party Protocols*, In Proceedings of CRYPTO 2008, LNCS 5157, 2008, pp.379 - 396.
28. Ore, O. *The General Chinese Remainder Theorem*, The American Mathematical Monthly, 59:6, 365-370, DOI: 10.1080/00029890.1952.11988142
29. Regev, O.: *On lattices, learning with errors, random linear codes, and cryptography*, In Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing, STOC 2005, pp. 84 - 93.
30. Regev, O.: *Lattice-based cryptography*, In Advances in Cryptology-CRYPTO, Springer, 2006, pp. 131-141.
31. Sen, J.: *Homomorphic Encryption: Theory & Application*, available at https://arxiv.org/abs/1305.5886.
32. Shor, P.W.: *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing, Volume 26 Issue 5, 1997, pp. 1484 - 1509.
33. Smart, N., Vercauteren, F. *Fully homomorphic encryption with relatively small key and ciphertext sizes*, In P. Nguyen and D. Pointcheval, editors, Public Key Cryptography, vol. 6056 of Lecture Notes in Computer Science, Springer, 2010, pp. 420 - 443.