COMPUTING PRIMITIVE IDEMPOTENTS IN FINITE COMMUTATIVE RINGS AND APPLICATIONS

MUGUREL BARCAU AND VICENŢIU PAŞOL

Abstract. In this paper, we compute an algebraic decomposition of black-box rings in the generic ring model. More precisely, we explicitly decompose a black-box ring as a direct product of a nilpotent black-box ring and local Artinian black-box rings, by computing all its primitive idempotents. The algorithm presented in this paper uses quantum subroutines for the computation of the p-power parts of a black-box ring and then classical algorithms for the computation of the corresponding primitive idempotents. As a by-product, we get that the reduction of a black-box ring is also a black-box ring. The first application of this decomposition is an extension of the work of Maurer and Raub [26] on representation problem in black-box finite fields to the case of reduced p-power black-box rings. Another important application is an IND-CCA[1] attack for any ring homomorphic encryption scheme in the generic ring model. Moreover, when the plaintext space is a finite reduced black-box ring, we present a plaintext-recovery attack based on representation problem in black-box prime fields. In particular, if the ciphertext space has smooth characteristic, the plaintext-recovery attack is effectively computable in the generic ring model.

1. Introduction

Many researchers have used for more than 20 years algorithms in generic models as a tool in proving reductions for hardness assumptions. These assumptions represent the foundation on which the security of public key encryption schemes is built. Working in generic models is difficult since all the computations are done by an oracle and very little information is available to the user besides abstract manipulation. Shoup introduced the generic group model in his 1997 seminal paper [30]. Therein and since then, a variety of cryptographic problems have been proven to be computationally intractable in the generic group model, most notably the Discrete Logarithm problem, the computational Diffie-Hellman problem [30], as well as the RSA problem over groups of hidden order [17].

Similarly, generic ring models are used to analyze the hardness of computational problems defined over rings. For example, it is proved in [23] that computing the Jacobi symbol of an integer is equivalent to factoring in the generic ring model, thus providing an example of a natural computational problem which is hard in the generic ring model but is feasible in the standard model. On the other hand, Aggarwal and Maurer proved in [4] that breaking RSA is equivalent to factoring in the generic ring model.

In the generic model, the more you know about the structure that the oracle computes, the better are the chances to produce algorithms that solve a specific

Key words and phrases. generic ring model; black-box rings; primitive idempotents; quantum computing; homomorphic encryption schemes.

problem. In this work, we provide algorithms in the generic ring model that compute the structure of a general ring, thus giving important information to the user. We also provide concrete applications of our results, which, due to their generic nature, they can be applied in a plethora of other applications.

Concretely, in the generic ring model, the representation of a ring is given by an oracle which outputs for an element a string of bits of a certain size; this representation gives no information about the algebraic structure but only an idea about its size. The algebraic computations are also performed by an oracle. If a set of generators for the ring is given, then the ring structure is called *black-box ring*, or BBR for short. We shall prove that a BBR can be explicitly decomposed as a product of a nilpotent ring with a unitary ring. Moreover, by the general theory of finite commutative unitary rings, one knows that any such ring is isomorphic to a product of local Artinian rings (each of the local Artinian factors is endowed with a BBR structure). The main scope of the paper is to provide an algorithm that computes this decomposition. This algorithm uses certain quantum subroutines that shall be explicitly mentioned. Concretely, we prove the following:

Theorem 1. *Let R be a commutative black-box ring.*

(1) *There exists a polynomial time quantum algorithm that explicitly computes an isomorphism of BBR's:*

$$R \simeq N_R \times \prod_p R_p,$$

where N_R is a nilpotent BBR and each R_p is a p-power BBR with unity (the product is over a finite set of primes).

(2) *If R is a p-power BBR with unity, there exists a classical polynomial time algorithm that explicitly computes an isomorphism of BBR's:*

$$R \simeq \prod_i R_i,$$

where for each i, R_i is a local Artinian ring.

We do so by explicitly computing all primitive idempotents of a BBR (see Theorem 7). The most involved part is the computation of the primitive idempotents in the case when R is a unitary commutative BBR with all its residual fields isomorphic to a fixed finite field $\mathbb{F}_q$ (Section 5.4). We proceed by reducing to the case where R is a product of isomorphic finite fields (Proposition 5). Furthermore, we prove first our result in the prime field case using an algorithm which produces with positive probability orthogonal idempotents. By iterating the process, with overwhelming probability, we produce the set of all primitive idempotents. The general case is reduced to the prime field case using an algorithm based on the trace map and the dual basis.

To present the applications of our main result we say a few words about fully homomorphic encryption (FHE). This is one of the most important and desired tools of modern cryptography, that allows evaluation of arbitrarily complex programs on encrypted data, while the data remains encrypted. The notion was suggested by Rivest, Adleman and Dertouzos in [27], where it was called "privacy homomorphism".

Any efficient FHE scheme would have a large number of practical applications such as: medical applications, financial privacy, consumer privacy in advertising, forensic image recognition, etc. (see [2]).

In [18], C. Gentry came up with the first concrete 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 plain data via 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 ([19], [15], [31], [14], [20]) was constructed following Gentry's recipe.

A second generation of fully homomorphic encryption schemes started in [9], where fully homomorphic encryption was established in a simpler way, based on the learning with errors assumption; the scheme was then improved in [11]. Currently, perhaps the arguably simplest FHE scheme based on the learning with errors assumption is by Brakerski [10] who builded on Regev's public key encryption scheme [28]. The latest advancement in this direction was obtained in [21], where a third generation of FHE scheme was constructed, achieving great leaps in efficiency.

Another very recent approach aiming for producing FHE was presented in [16], where the authors based their construction on the finite field isomorphism problem. All the schemes considered above are based on the method of constructing a noisy version of the ciphertext (the noise is added to guarantee the security of the cryptosystem). For this reason, these schemes are called noisy FHE schemes.

In this respect, an important and natural question would be whether one can actually construct a noise-free FHE scheme (see C. Gentry's talk at ICM 2022). A possible approach towards noise-free FHE schemes 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. Such a scenario has been considered before by other authors (see for example [25], p.4). Unfortunately, there are no secure examples of such primitives in the literature and the results of this paper may explain why they are hard to find. It is worth mentioning that in the 1996 paper of Boneh and Lipton [8], an "algebraically homomorphic encryption scheme" is a ring homomorphic encryption scheme whose plaintext space is the ring of integers modulo some positive integer n and ciphertext space is a black-box ring. In the simplest case, the plaintext space is the prime field $\mathbb{F}_p$ while the ciphertext space is a black box field isomorphic to $\mathbb{F}_p$ via the decryption map. Consequently, the encryption map is a one-way permutation, so that the encryption algorithm is deterministic, which does not meet the today minimal security requirements such as IND-CPA security. It is shown in [26] that the isomorphism problem (i.e. the problem that inquires the existence of such one-way permutations) for finite extensions of $\mathbb{F}_p$ can be efficiently reduced to the representation problem for $\mathbb{F}_p$ (to represent an element of $\mathbb{F}_p$ means to write it as a polynomial expression, with integer coefficients, in a given set of generators). More precisely, the isomorphism problem for $\mathbb{F}_{p^k}$ is efficiently reducible to the representation problem for $\mathbb{F}_{p^k}$, which in turn is efficiently reducible to the representation problem for $\mathbb{F}_p$. We mention that the representation problem for $\mathbb{F}_p$ is an important open problem in cryptography (for more details see

[26]). As a first application of our main theorem, we extend this result to the case of a product of finite fields, all having the same characteristic p. To be precise, we show that the representation problem for such a product of fields is efficiently reducible to the representation problem for $\mathbb{F}_p$.

Another important application of our generic ring model algorithm for the computation of all primitive idempotents is a quantum-classical IND-CCA^1 attack for any ring homomorphic encryption scheme whose plaintext space is not a nilpotent ring. Moreover, under some assumptions on the plaintext space, we show that a plaintext-recovery attack can be constructed.

1.1. **Organization of the Paper.** Section 2 is dedicated to the representation of finite rings in the generic model; we introduce oracle and black-box rings.

The main theoretical results of this paper are presented in Section 3. Here, after presenting some preliminary results and notations, we prove the theoretical decomposition for (not necessarily unitary) commutative rings, and we study the properties of homomorphisms between finite commutative rings. Moreover, a Teichmüler lifting result is recalled in the case of finite commutative rings with isomorphic residual fields.

We start Section 4 by pointing out the algorithm for computing periods in semigroups using a modified Shor's quantum algorithm. This algorithm is applied for computing the idempotent map in finite commutative rings. For the case of p-power rings, we show that this map can be computed classically.

In Section 5 we describe the algorithms that compute the primitive idempotents in the generic ring model. We first compute the unitary part of a ring, then we show how to decompose a ring with unity as a product of p-power rings. The next step is to break further any p-power BBR into a product of rings, each of them having isomorphic residual fields. After we reduce the computation to the case where the ring is a product of isomorphic finite fields, we finally present a series of algorithms that compute the primitive idempotents of such a ring.

Finally, Section 6 presents 3 applications: an extension of a result of [26] on representation problem for finite fields to the case of a product of finite fields of equal characteristic. Then, we present a quantum-classical IND-CCA^1 attack on ring homomorphic encryption schemes over generic quasi-unital rings and, in the case of ring homomorphic encryption schemes over a reduced ring with smooth characteristic, we present a plaintext-recovery attack in the generic ring model.

Acknowledgements

We would like to express our gratitude to anonymous reviewers for their valuable comments, which greatly improved the earlier version of this paper.

2. Representing finite rings

From the practical point of view it is important to understand how one represents the elements of a finite ring. As we shall describe below, an element of a ring is given by a fixed length string of bits. The algebraic operations are assumed to be accessible, but not explicit (see the definition below). Basically, the only non trivial information that can be deduced about the ring (unless otherwise specified) is a bound for the number of elements in the ring and a representation for its neutral element for addition. In other words, no information about its algebraic structure

can be deduced from this representation. The following definition is inspired by the notions of black box groups (introduced by Babai and Szemerédi in [6]) and black box fields (introduced by Boneh and Lipton in [8]).

Definition 1. A *ringlike oracle* consists of two components: a validation oracle and a computational oracle. The validation oracle takes queries strings of length n over $\{0,1\}$ and outputs a validation bit. The computational oracle takes queries of the form $(x,y,+)$, $(x,-)$, $(x,y,\cdot)$, where x,y are valid strings and outputs a valid string. Moreover, the computational oracle outputs a valid string in response to the zero element query 0. We assume that every component of a ringlike oracle can be simulated by a deterministic polynomial (in the length n of the representation) time algorithm. An *oracle ring* is a ringlike oracle such that the set of valid strings together with the operations defined by the responses to the above queries forms a ring. An (n,d)-*black-box ring*, or BBR for short, is a subring of an oracle ring generated by a finite set of size d.

By a finite generating set of a (nonunital) ring R, we mean 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; however, this expression or its bit representation is not assumed to be known.

In order to show that a certain (abstract) ring R is an oracle ring, one needs to construct (or explicitly show the existence of) an oracle representation, i.e. an oracle as in Definition 1 for which the associated ring is isomorphic to R.

Notice that if R is an oracle ring and I is an ideal of R, one cannot in general realise R/I as an oracle ring. For example, let $I=Nil(R)$ be the nilradical of R. Although one can check (using the oracle of R) whether $x\in Nil(R)$ for any $x\in R$, there is no obvious way of realising $R^{red}:=R/Nil(R)$ as an oracle ring. The solution to this problem will be a key ingredient in our practical applications:

Theorem 2. *There is a quantum algorithm that on input an (n,d)-BBR R outputs a realization of R^{red} as an (n,d)-BBR. The algorithm runs in time polynomial in (n,d).*

We postpone the proof of this theorem until Section 5.3. The difficulty of the proof of this theorem is to realize R^{red} as an oracle ring, and to construct explicitly the canonical map $R\to R^{red}$. Once we do that, the image of the generating set of R can be taken as a set of generators for R^{red}, which will imply that R^{red} is indeed a BBR. In order to represent R^{red} as an oracle ring, we will need an explicit computation of the structure of the ring R (see Theorem 4). Then, we can use a Teichmüler-type lifting procedure to identify R^{red} with an explicit subset of R, thus R^{red} inherits the representation of R. Moreover, we modify the addition on this subset of R, so that the identification becomes an isomorphism of rings. This realizes R^{red} as an oracle ring. In addition, the procedure also outputs an explicit realization of the map $R\to R^{red}$.

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 that we need for our applications, we shall give all the necessary details.

3.1. **Preliminaries.** A commutative ring R is called *nilpotent* if there exist a positive integer n such that $x^n = 0$ for all $x \in R$. In the case of a finite commutative ring R, this is equivalent to the existence, for any $x \in R$, of a positive integer m (that may depend on x) such that $x^m = 0$. We say that a finite commutative ring is *quasi-unital* if it is not nilpotent; equivalently, its unital subring is non-trivial (see Theorem 3).

If R is a commutative ring, then $x \in R$ is called an *idempotent* whenever $x^2 = x$. Moreover, $x \in R$ is called a *primitive idempotent* if x is a nonzero idempotent which cannot be written as a sum of two orthogonal nonzero idempotents, i.e. if $x = e_1 + e_2$ with $e_1^2 = e_1$, $e_2^2 = e_2$, and $e_1 \cdot e_2 = 0$, then either $e_1 = 0$ or $e_2 = 0$.

If R is a commutative ring then we denote by $E(R) := \{e \in R \mid e^2 = e\}$ 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 the idempotent $\mathbb{F}_2$-algebra of R. It is shown in [7], that if R is a finite commutative ring then there is a well defined map $\mathbf{e} : R \to E(R)$, that is a homomorphism of multiplicative semigroups. More precisely, for $x \in R$, the sequence $\{x^n\}_{n \geq 1}$ is eventually periodic. If we denote by $p(x)$ the period and by $t(x)$ the tail, then $x^{k \cdot p(x)}$ is an idempotent for all k with $k \cdot p(x) \geq t(x)$ (for more details see [7]). We shall denote by $\mathbf{e}(x)$ this idempotent. In fact, this is the unique idempotent belonging to the sequence (indeed, if $e_1 = x^{m_1}$ and $e_2 = x^{m_2}$ are two idempotents in the sequence, then $e_1 = e_1^{m_2} = x^{m_1 m_2} = e_2^{m_1} = e_2$) . Notice that a finite commutative ring R is nilpotent if and only if $E(R) = \{0\}$. We need the following lemmata:

Lemma 1. *In a commutative ring R any two distinct primitive idempotents are orthogonal.*

Proof. Let e, f be two distinct primitive idempotents. Suppose that $e \cdot f \neq 0$. Since $e = ef \oplus (e \oplus ef)$ and $e \neq e \oplus ef$, we get that $e = ef$. Similarly, $f = ef$ so that $e = f$, which is a contradiction. □

Lemma 2. *In any quasi-unital ring R there exists primitive idempotents.*

Proof. We have seen that $E(R)$ is non-trivial. Let $f \in E(R)$ be a nonzero idempotent. If f is primitive, we are done. Otherwise, one can write f as a finite sum of mutually orthogonal (hence distinct) nonzero idempotents (since f is not primitive such a sum with two terms exists). Now, choose such a sum $f = e_1 + \ldots + e_k, k \geq 2$ of maximal possible length (this is possible because R is a finite ring). We prove that e_i is a primitive idempotent for all i. Suppose the contrary, then for some i we have $e_i = e_{i,1} + e_{i,2}$, where $e_{i,1}, e_{i,2}$ are orthogonal nonzero idempotents. For $j \neq i$ we have $e_j \cdot e_{i,1} = e_j \cdot e_i \cdot e_{i,1} = 0$. Similarly, $e_j \cdot e_{i,2} = 0$. Hence we can write

$$f = e_1 + ... + e_{i-1} + e_{i,1} + e_{i,2} + e_{i+1} + ... + e_k,$$

as a sum of $k + 1$ mutually orthogonal idempotents, contradicting the maximality of k. □

Remark 1. In the above proof, we actually showed that any nonzero idempotent can be represented as a finite sum of primitive idempotents. In fact, such a representation is unique (up to permutations). Indeed, let $f = e_1 + ... + e_k$, where e_i is a primitive idempotent for all i. Let e be a primitive idempotent, since by Lemma 1 e is orthogonal to any other primitive idempotent, we get that $e \cdot f = 0$ if $e \neq e_i$ for all i, and $e \cdot f = e$ otherwise; which proves the uniqueness. Moreover, the last argument shows that the unity (if it exists) is the sum of all primitive idempotents.

The above remark motivates the following definition:

Definition 2. For any nonzero idempotent f we define its *support* by:

$$Supp\{f\} := \{e \mid e \cdot f = e \text{ and } e \text{ is a primitive idempotent}\}.$$

For any idempotent f, the equality (shown in Remark 1):

$$f = \sum_{e \in Supp\{f\}} e,$$

shall be called the *primitive representation* of f.

We recall the following result from [7], Proposition 4:

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).

By Remark 1, if $\{e_1, ..., e_k\}$ is the set of primitive idempotents of R then $E(R) \simeq \bigoplus_i \mathbb{F}_2 \cdot e_i$ as $\mathbb{F}_2-$algebras. The second assertion follows immediately by observing that there exists a unique primitive idempotent which is sent by ϕ to 1.

Remark 2. If R is a finite commutative ring *with unity* then it is an Artinian ring, and the structure theorem for Artinian rings (Theorem 8.7 in [5]) asserts that R is isomorphic to a product $R_1 \times ... \times R_n$ of local Artinian rings. This isomorphism gives rise to

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

Last proposition shows that even in the case of a non-unital ring R, the idempotent algebra is isomorphic to $\mathbb{F}_2^n$. If R is a ring with unity, since $1 = e_1 + ... + e_n$, where $e_1, ..., e_n$ are the primitive idempotents of R, then the map $R \to \prod_i Re_i$, $x \mapsto (xe_1, ..., xe_n)$ is an isomorphism, so that the rings R_i are in fact isomorphic to the rings Re_i. In particular, the number of local Artinian rings that appear in the decomposition of R is equal to the number of its primitive idempotents (for more details see [7]).

We end this section with the following useful lemmas about BBR structures.

Lemma 3. *Let R be a commutative $(n, d)-$BBR and e be an idempotent (given by its binary representation). Then, the ring $S := Re$ is a commutative $(n, d)-$BBR.*

Proof. The ring S inherits the oracle ring structure from R. The validation component of the oracle structure of S checks first the validity of x using the validation component of the oracle structure of R and then checks the equality $x = x \cdot e$. The computational component of the oracle structure of S uses the computational component of the oracle structure of R. It is clear that the computational complexity of the oracle of S remains polynomial in the length of the representation. Finally, if $G = \{g_1, ..., g_d\}$ is a set of generators of R, then $Ge := \{g_1 e, ..., g_d e\}$ is a generating set of S. □

Lemma 4. *Let $R_i, i \in \overline{1,k}$ be a finite set of $(n_i, d_i)-BBRs$. Then, the product $\prod_{i=1}^{n} R_i$ is a $(\sum_i n_i, \sum_i d_i)-BBR$.*

Proof. Using string concatenation, it is easy to see that such a product of oracle rings is an oracle ring. The union of all generating sets (viewed inside the product) is a set of generators for the product. □

3.2. **Structural theorem.** The aim of this section is the following:

Theorem 3. *Any finite commutative ring is a product of a unital subring and a nilpotent subring. Moreover, the decomposition is unique.*

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 nilradical 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. We prove below the following explicit version of the first part of Theorem 3:

Theorem 4. *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.*
2. *The map $R \to \bar{R} \times N_R$, $x \mapsto (x\bar{e}, x - x\bar{e})$ is a ring isomorphism.*
3. *Any morphism of rings $S \to R$ with S unital, factors through $S \to \bar{R} \subseteq R$.*

Proof. (1) The fact that $\bar{R}$ is a unital ring is clear. The unit is $\bar{e}$, because $x\bar{e} \cdot \bar{e} = x\bar{e}$, $\forall x\bar{e} \in \bar{R}$. It is clear that $\bar{e}$ is also the unit in $E(R)$. The equality $x \cdot \bar{e} = 0$ yields $x^n \cdot \bar{e} = 0$ for any positive integer n, so that $\mathbf{e}(x) \cdot \bar{e} = 0$. But now the identity takes place in $E(R)$ where $\bar{e}$ is the unit, thus $\mathbf{e}(x) = 0$, which implies 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) Let $\phi : S \to R$ be a morphism of rings with S unital. 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 3. 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 of the forgetful functor $\overline{CRings} \to CRngs$, given by forgetting the multiplicative identity. The proof of (3) from Theorem 4 shows the right adjointness.

Proof of Theorem 3. By the previous theorem it remains to show the unicity of the decomposition in Theorem 3. Let $R = R_1 \times R_2$ 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 $R_2 = N_R$. □

3.3. **Homomorphisms.** The following results describe ring homomorphisms from a ring to a local ring.

Theorem 5. *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 primitive idempotent $e \in R$ such that $\varphi(e) \neq 0$. Of course, $\varphi(e) = 1$. Using the explicit decomposition Theorem 4, we conclude that, indeed, φ factors through the projection $R \to Re$. □

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, for any ring homomorphism $\varphi : R \to k$, 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. □

3.4. **Teichmüler liftings.** The following result is known to specialists and establishes the existence of Teichmüler liftings. We express it in a very explicit way that shall be used in our applications. Throughout the paper a local ring is assumed to be a commutative ring with unity.

Theorem 6. *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 $y \in R$ is such that $y \bmod \mathfrak{m} = \bar{x}$, then $y^{q^r} = x$ for any r with $\mathfrak{m}^r = (0)$.*

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 $y_1 \equiv y \bmod \mathfrak{m}$, 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 $y_r = y_{r-1}$ for any r such that $\mathfrak{m}^r = (0)$. Denoting by x this stationary value, we get that $x^q = x$ and $x \equiv y \mod \mathfrak{m}$. □

Remark 4. Under the conditions of Theorem 6, we have: $\mathbf{e}(y) = y^{q^r(q-1)} \in \{0_R, 1_R\}$. Indeed, since the residue field k has size q, we have that $y^{q-1} \bmod \mathfrak{m} \in \{0_k, 1_k\}$. Now, using the last theorem we get that $y^{q^r(q-1)} \in \{0_R, 1_R\}$.

We have the following useful consequence of Theorem 6 :

Corollary 2. Let $(R, \mathfrak{m})$ be a local ring and let $S := \{x \in R | x^q = x\}$. Then $(S, +_S, \cdot)$ is isomorphic to the residue field $R/\mathfrak{m}$, where $x +_S y = (x + y)^{q^r}$, and $\cdot$ is the usual multiplication on R (here q is the size of the residue field $R/\mathfrak{m}$, and r is the nilpotency index of the maximal ideal).

Proof. Let $\pi : R \to R/\mathfrak{m}$ be the projection map. By Theorem 6 the restriction of π to S is a bijection; let $\rho : R/\mathfrak{m} \to S$ be the inverse map. Then, $x +_S y = \rho(\pi(x) + \pi(y))$ and $x \cdot y = \rho(\pi(x) \cdot \pi(y))$ for all $x, y \in S$, which shows that $\pi : (S, +_S, \cdot) \to (R/\mathfrak{m}, +, \cdot)$ is a ring isomorphism. □

Definition 3. 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 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 having residue fields isomorphic to $\mathbb{F}_{p^k}$. When $R = R_p$, we say that R is a *p-power ring*.

Corollary 3. If R is a p-power (n, d)-BBR whose Artinian local rings have residue fields isomorphic to a fixed finite field $\mathbb{F}_q$, then R^{red} is an (n, d)-BBR.

Proof. As in Corollary 2, let $S = \{x \in R | x^q = x\}$. Let $R = \prod_i Re_i$, where $(Re_i, \mathfrak{m}_i)$ are its local Artinian components and let S_i be the corresponding subsets of Re_i as in Corollary 2. Then $S_i = S \cdot e_i$ and $S = \prod_i S_i$. As above, on S we define addition by the formula $x +_S y = (x + y)^{q^r}$, where r is the nilpotency index of the ideal $\prod_i \mathfrak{m}_i$ (one can take $r = \lfloor \log_q |R| \rfloor$, see the proof of Proposition 3). Then $(S, +_S, \cdot)$ becomes a ring isomorphic to $\prod_i (S_i, +_{S_i}, \cdot)$, which by Corollary 2, is isomorphic to $\prod_i Re_i/\mathfrak{m}_i$ (the fact that $S = \prod_i S_i$ and each $(S_i, +_{S_i}, \cdot)$ is a ring shows that $(S, +_S, \cdot)$ is a ring) . Since the latter ring is isomorphic to R^{red}, as an abstract ring, we get that $S \simeq R^{red}$. Now it remains to describe the BBR structure of S.

The validation oracle checks for valid strings x that satisfy $x^q = x$. The computational component of the oracle of S uses the computational component of R to compute $(\cdot)$, respectively $(+_S)$ as described above. Remark that, raising to the power q^r can be computed in $O((\log_2(q^r))^2)$ time, and since one can take $r = \lfloor \log_q |R| \rfloor$ we get $O(n^2)$. Finally, since the composition map $\rho \circ \pi : R \to R^{red} \to S$ is a surjective ring homomorphism, if $G = \{g_1, ..., g_d\}$ is a set of generators for R then $G^{red} := \{g_1^{q^r}, ..., g_d^{q^r}\}$ is a set of generators for S. Consequently, we realised R^{red} as an (n, d)-BBR. □

4. Computing the map **e**

In general, there is no polynomial time algorithm that computes the map $\mathbf{e} : R \to E(R)$. This can be done using quantum computations as we shall present below. However, if one knows some additional information about the structure of the ring, then no quantum computations are required (for example in the case of p-power rings).

The next result was presented in [12] (see also [13, 7]), and is an adaptation of Shor's algorithm (see [29]).

Proposition 2. There is a *quantum algorithm* that on input (G, g), where G is an oracle semigroup of length n representation and $g \in G$ is an element, outputs the period $p(g)$ in time polynomial in n.

Remark 5. An *oracle semigroup* is a semigroup whose elements are encoded by bit strings of length n, and the semigroup operation is performed by an oracle. The authors of [12] use the notion of black-box semigroup instead of oracle semigroup. To be consistent to our definitions of oracle/black-box rings in Definition 1, a black-box semigroup would be an oracle semigroup furnished with a finite set of generators. However, in the above result, one does not need a set of generators for the semigroup G.

Corollary 4. There is a *quantum algorithm* that on input a commutative oracle ring R and an element $x \in R$, outputs $\mathbf{e}(x)$ in time polynomial in the length of the representation of R.

Proof. Using Proposition 2 one finds first $p(g)$ and then compute $k := \left\lceil \frac{|R|}{p(g)} \right\rceil$. Now, compute $\mathbf{e}(g) = g^{kp(g)}$. Since $kp(g) \leq 2|R|$ we get that the complexity is polynomial in $\log_2 |R| \leq n$. □

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

Proposition 3. There is a *classical algorithm* that on input a p-power oracle ring R and an element $x \in R$, outputs $\mathbf{e}(x)$ in time polynomial in the length of the representation of R.

Proof. We show first that the map $\mathbf{e}$ can be computed using the following formula:

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

Let $R = R_1 \times ... \times R_m$, 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 $y = (y_1, ..., y_m)$, then by Remark 4 and Remark 2, we obtain that

$$\begin{aligned} \mathbf{e}(y) &= (\mathbf{e}(y_1), ..., \mathbf{e}(y_m)) = (y_1^{p^{k_1 N_1}(p^{k_1}-1)}, ..., y_m^{p^{k_m N_m}(p^{k_m}-1)}) \\ &= y^{p^{\max_i\{k_i N_i\}}(p-1)(p^2-1)...(p^{\max_i\{k_i\}}-1)}. \end{aligned}$$

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 (non-trivial) $\mathbb{F}_{p^{k_i}}$-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 $k_i \leq k_i N_i \leq \log_p |R|$ so that

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

We can efficiently evaluate $\mathbf{e}(y)$ by using the square-and-multiply techniques. More precisely, we need at most $(\log_2 |R|)^4$ multiplications. □

5. Computing the primitive idempotents of a ring

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

Theorem 7. *There is a probabilistic algorithm that on input R, a commutative (n,d)-BBR, outputs all its primitive idempotents in time polynomial in (n,d).*

Recall that by Theorem 4 we have a decomposition $R \simeq \bar{R} \times N_R$, and by Artin decomposition theorem (see also Remark 2) $\bar{R} \simeq \prod_i \bar{R}e_i$, where e_i are the primitive idempotents of R. Since $\bar{R}e_i = Re_i$, we get that $R \simeq \prod_i Re_i \times N_R$. We note that the above theorem gives an explicit way for the computation of this decomposition of R. Our strategy runs as follows:

(1) We first exhibit the unital part of a ring R by computing $\bar{e}_R$.
(2) For a unital ring R, we single out a set of primes $\mathcal{P}$ and a set of idempotents $\{e_p \mid p \in \mathcal{P}\}$ such that $R \simeq \prod_p Re_p$, and Re_p is a p-power ring.
(3) For a unital p-power ring R, we compute a finite set of integers $S \subseteq \mathbb{Z}_{>0}$ and a set of idempotents $\{e_{p,k} \mid k \in S\}$ such that $Re_{p,k}$ is a unital subring of R whose residue fields are all isomorphic to $\mathbb{F}_{p^k}$ and $R \simeq \prod_{k\in S} Re_{p,k}$.
(4) Finally, for a unital ring R, whose residue fields are all isomorphic to $\mathbb{F}_{p^k}$, we compute its primitive idempotents.

Remark 6. Quantum computation is used only to determine N_R and each e_p (with p prime), i.e. for steps (1) and (2). For the other two steps: (3) and (4), only classical computation is needed.

5.1. **Computing the unital part.** Let R be a non-unital commutative (n,d)-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 $\{e_1, \dots e_m\}$ 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 8. *Let $G = \{g_1, \dots, g_d\}$ be the generating set of a quasi-unital ring R. Then*

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

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

Proof. Let $R_k = Re_k$, $k \in \overline{1,m}$ be the local Artinian components of R, and let $\mathfrak{m}_k$ be their maximal ideals. It is enough to show that, for any k, 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 the kernel of the following composition of homomorphisms:

$$R \to \bar{R} \to R_k \to R_k/\mathfrak{m}_k,$$

which is a proper ideal of R, and this is impossible. □

As a consequence we have the following:

Proposition 4. There is a *quantum algorithm* that takes as input an (n,d)-BBR R and outputs the unity of its unital part in time polynomial in (n,d).

Proof. Since by Corollary 4, $\mathbf{e}(g_j)$ can be computed in time polynomial in n, the conclusion follows by the formula for $\bar{e}$ exhibited in Theorem 8. □

By Lemma 3, if R is an (n,d)-BBR then $\bar{R}$ is an (n,d)-BBR. Since $\bar{R}$ is a unital ring, we may assume from now on that R is a unital commutative BBR. This ends step (1) of our strategy.

5.2. **Computing the p-power parts of a unital ring.** The purpose of this subsection is to show how to compute the decomposition of a unital commutative ring into its $p-$power parts, where p is a prime number. Since we don't need a system of generators for this decomposition, the next result is valid in the more general context of unital commutative oracle rings.

Theorem 9. *There is a quantum algorithm that on input a unital commutative oracle ring R together with the binary representation of its unit outputs a set of primes $\mathcal{P}$ and a set of idempotents $\{e_p \mid p \in \mathcal{P}\}$ such that $R \simeq \prod_p Re_p$, and Re_p is a p-power ring. The algorithm runs in time polynomial in the length of the representation of R. Moreover, if R is an (n,d)-BBR then each ring Re_p is a unital p-power (n,d)-BBR.*

Proof. The algorithm is divided in the following subroutines:

- Use Shor's quantum algorithm to compute the characteristic of R, which is the additive period of 1_R, i.e. the minimal positive integer N such that $N \cdot 1_R = 0$ (see Proposition 2).
- Use Shor's quantum factoring algorithm to compute the prime factorization of $N = \prod_p p^{\alpha_p}$ (see [29]). Set $\mathcal{P} := \{p \mid \alpha_p \geq 1\}$.
- Use the extended Euclidean algorithm to compute integers $\{u_p\}_{p\in\mathcal{P}}$ such that $\frac{N}{p^{\alpha_p}} \mid u_p$ and $\sum_p u_p = 1$.
- Set $e_p := u_p \cdot 1_R$.
- Output $\mathcal{P}$ and $\{e_p \mid p \in \mathcal{P}\}$.

Notice that all of the above subroutines of the algorithm run in time polynomial in the length representation of R. From $\sum_p u_p = 1$ and $p^{\alpha_p} \mid u_q$ for $q \neq p$ we deduce that $p^{\alpha_p} \mid (1-u_p)$, hence $N \mid u_p(1-u_p)$. This shows that $e_p - e_p^2 = (u_p - u_p^2)\cdot 1_R = 0$, i.e. e_p is an idempotent for each p. For distinct $p, q \in \mathcal{P}$ we have that $u_p \cdot u_q$ is divisible by the product $\frac{N}{p^{\alpha_p}} \cdot \frac{N}{q^{\alpha_q}} = N \cdot \frac{N}{p^{\alpha_p} q^{\alpha_q}}$, hence by N. Since $N \cdot 1_R = 0$, we get that $e_p \cdot e_q = u_p u_q \cdot 1_R = 0$. Moreover, since $\sum_p u_p = 1$ we get that $\sum_p e_p = 1_R$, therefore $R \simeq \prod_p Re_p$. Notice that the additive period of e_p is p^{α_p} so that any residue field of Re_p has characteristic p, therefore Re_p is a p-power ring for each $p \in \mathcal{P}$. Finally, the last assertion of the theorem is an immediate consequence of Lemma 3. □

This ends step (2) of our strategy so that from now on we may assume that R is a p-power BBR. As mentioned in Remark 6 all the remaining subroutines are classical.

5.3. **Computing the idempotents $e_{p,k}$.** Step (3) is achieved in the following:

Theorem 10. *There is a classical algorithm which takes as input a p-power (n,d)-BBR R and outputs a finite set of integers $T_p \subseteq \mathbb{Z}_{>0}$ and a set of idempotents $\{e_{p,k} \mid k \in T_p\}$ such that $Re_{p,k}$ is a unital subring of R, whose residue fields are all isomorphic to $\mathbb{F}_{p^k}$, and $R \simeq \prod_{k\in T_p} Re_{p,k}$. The algorithm runs in time polynomial in (n,d).*

Proof. Let $G = \{g_1, \ldots, g_d\}$ be a set of generators for the ring R. The algorithm runs as follows:

Algorithm 1: Compute $e_{p,k}$

$\bar{e}_{p,0} := 1_R$
$T_p = \emptyset$; $E = \emptyset$
$k = 0$
while $\bar{e}_{p,k} \neq 0$
$k = k + 1$
    for $i = 1$ to d **do**
        $\mathfrak{e}_{i,k} := \mathbf{e}(g_i \cdot \bar{e}_{p,k-1} - g_i^{p^k} \cdot \bar{e}_{p,k-1})$
    end for
$\bar{e}_{p,k} = \bigvee_{i=1}^{d} \mathfrak{e}_{i,k}$
$e_{p,k} = \bar{e}_{p,k-1} - \bar{e}_{p,k}$
    If $e_{p,k} \neq 0$ **then**
        $T_p = T_p \cup \{k\}$
        $E = E \cup \{e_{p.k}\}$
    end if
end while
return T_p, E

Let us note first that the algorithm terminates for some k smaller or equal to n. Indeed, if $e_{p,k} \neq 0$ for some k then, since $Re_{p,k}$ is a subring of R we get that $|Re_{p,k}| \leq |R|$. On the other hand, any residue field of $Re_{p,k}$ has size at most the size of $Re_{p,k}$, i.e. $p^k \leq |Re_{p,k}| \leq |R| \leq 2^n$ so that $k \leq n$. It is clear that algorithm runs in time polynomial in (n,d).

We need to show that, for each $k \geq 1$, all residue fields of the local Artinian components of $Re_{p,k}$ are isomorphic to $\mathbb{F}_{p^k}$. For this, it is enough to prove by induction on k that $\bar{e}_{p,k}$ is the sum of all primitive idempotents whose residue fields are isomorphic to $\mathbb{F}_{p^m}$ with $m \geq k+1$. The case $k = 0$ follows from Remark 1. Since the computation of $\bar{e}_{p,k}$ takes place in $R\bar{e}_{p,k-1}$ and using the step of induction, we get that $\bar{e}_{p,k}$ is a sum of primitive idempotents whose residue fields are of size at least p^k. We show first that a primitive idempotent f with residue field of size p^k does not occur in the primitive decomposition of $\bar{e}_{p,k}$. Assuming the contrary, then there exist an $i \in \overline{1,d}$ such that $\mathfrak{e}_{i,k} \cdot f = f$, equivalently $\mathbf{e}(g_i \cdot f - g_i^{p^k} \cdot f) = f$.

On the other hand, since the residue field of Rf is $\mathbb{F}_{p^k}$ we have that $g_i f \equiv (g_i f)^{p^k} = g_i^{p^k} f \mod \mathfrak{m}_f$, so that

$$0 = \mathbf{e}(g_i f - g_i^{p^k} f) = \mathbf{e}(g_i - g_i^{p^k}) f = f,$$

which is a contradiction (here $\mathfrak{m}_f$ is the maximal ideal of the local Artinian ring Rf). Hence $\bar{e}_{p,k}$ is a sum of primitive idempotents with corresponding residue fields isomorphic to $\mathbb{F}_{p^m}$ with $m > k$. Moreover, $\bar{e}_{p,k}$ is the sum of all primitive idempotents with corresponding residue fields isomorphic to $\mathbb{F}_{p^m}$ for some $m > k$. Let f be a primitive idempotent with corresponding residue field isomorphic to $\mathbb{F}_{p^m}$ for some $m > k$. Since $\{g_1 f \mod \mathfrak{m}_f, ..., g_d f \mod \mathfrak{m}_f\}$ generates $Rf/\mathfrak{m}_f$ and $Rf/\mathfrak{m}_f$ is isomorphic to $\mathbb{F}_{p^m}$ for some $m > k$, there exist an i such that $g_i e - (g_i e)^{p^k} \notin \mathfrak{m}_f$ (otherwise the set $\{g_1 f \mod \mathfrak{m}_f, ..., g_d f \mod \mathfrak{m}_f\}$ is a subset of $\mathbb{F}_{p^{\gcd(k,m)}}$, which is a strict subfield of $\mathbb{F}_{p^m}$). Therefore, we get that $\mathbf{e}(g_i - g_i^{p^k})f = f$, which proves our claim. In particular, we proved that $Re_{p,k} = R_{p,k}$ as in Definition 3.

Since 1_R is the sum of all primitive idempotents and each one of them occurs in the primitive decomposition of exactly one of the $e_{p,k}$'s, we get that $\sum_k e_{p,k} = 1_R$ and any two $e_{p,k}$'s are orthogonal. In particular, this proves that $R \simeq \prod_{k \in T_p} Re_{p,k}$. □

Now we have all the necessary ingredients to give the proof of Theorem 2.

Proof of Theorem 2. : We recall that there is a quantum algorithm that on input R, a commutative (n, d)-BBR, outputs a realization of $\bar{R}$ as a commutative (n, d)-BBR (Proposition 4, Lemma 3). Since $R^{red} \simeq \bar{R}^{red}$ as rings, we may assume that R is a unital (n, d)-BBR. By Theorems 9 and 10 there is a quantum algorithm that on input a unital commutative (n, d)-BBR outputs a set of primes $\mathcal{P}$, a set of positive integers T_p for each $p \in \mathcal{P}$, and a set of idempotents $\{e_{p.k} \mid p \in \mathcal{P}, k \in T_p\}$ such that $R \simeq \prod_{p,k} Re_{p,k}$ and all the residue fields of $Re_{p,k}$ are isomorphic to $\mathbb{F}_{p^k}$.

Recall from Corollary 3 that, for each pair (p, k), the following subset of R

$$S_{p,k} = \{x \in Re_{p,k} \mid x^{p^k} = x\},$$

together with $x +_{p,k} y = (x + y)^{p^{kn}}$ and $x \cdot_{p,k} y = x \cdot y$ is a ring oracle structure for $(Re_{p,k})^{red}$. Consider now the following subset of R:

$$S = \{x \in R \mid (x \cdot e_{p,k})^{p^k} = x \cdot e_{p,k} \; \forall p \in \mathcal{P}, \forall k \in T_p\}.$$

Observe that the map $S \to \prod_{p,k} S_{p,k}$ defined by $x \mapsto (x \cdot e_{p,k})_{p \in \mathcal{P}, k \in T_p}$ is a bijection with inverse $(x_{p.k})_{p \in \mathcal{P}, k \in T_p} \mapsto \sum_{p.k} x_{p,k}$. This bijection becomes an isomorphism of rings if we endow S with the following ring structure: $x \cdot_S y := x \cdot y$ (the usual multiplication on R), while $x +_S y := \sum_{p,k}(x \cdot e_{p,k} +_{p,k} y \cdot e_{p,k})$.

Since $R \simeq \prod_{p,k} Re_{p,k}$, we have that $R^{red} \simeq \prod_{p,k}(Re_{p,k})^{red} \simeq \prod_{p,k} S_{p,k} \simeq S$. Therefore S is an oracle ring realization of R^{red}. In particular, the length of the representation is n. Let $\{g_1, ..., g_d\}$ be a set of generators for R, then the set $\{h_1, ..., h_d\}$ with $h_i := \sum_{p,k}(g_i e_{p,k})^{p^{kn}}$, $\forall i \in \overline{1, d}$ is a set of generators for S, due to the surjectivity of the ring homomorphism $R \to R^{red}$. This shows that R^{red} is an (n, d)-BBR. □

5.4. **Computing the primitive idempotents.** Step (3) of our strategy was completed in the previous subsection. It remains to discuss the last step, that is to show how to compute the primitive idempotents of a p-power (n, d)-BBR R whose residue fields are all isomorphic to $\mathbb{F}_q = \mathbb{F}_{p^k}$. According to the next proposition we can work with R^{red}, instead of R. Indeed, we have the following result:

Proposition 5. Let R be a p-power ring (n,d)-BBR whose residue fields are all isomorphic to a fixed finite field $\mathbb{F}_q$, and let S be the (n,d)-BBR as in Corollary 3, then R and S have the same primitive idempotents.

Proof. Let e be an idempotent of R, then since $e^q = e$ we have that $e \in S$ and in addition e is also an idempotent of S because the multiplication in S coincides with the multiplication of R. The converse also holds trivially. Since the two sets of idempotents have the same cardinality, we deduce that R and S have the same number of primitive idempotents (see Proposition 1). To close the proof we show that any primitive idempotent of R is also a primitive idempotent of S. Let e be a primitive idempotent of R. Suppose that e is not a primitive idempotent of S. Then we can write e as $e = e_1 +_S e_2$ with $e_1 \cdot e_2 = 0$, where e_1, e_2 are idempotents of S, hence also of R. We obtain that $e = (e_1 + e_2)^{q^n} = e_1 + e_2$, which yields that either $e_1 = 0$ or $e_2 = 0$, because e is a primitive idempotent of R. □

As a consequence, throughout the rest of this section we assume additionally that R is a reduced ring, hence R is a product of isomorphic finite fields.

5.4.1. *Computing the primitive idempotents when $k = 1$.* We are in the case $R \simeq \prod_i Re_i$ 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. $R \simeq \mathbb{F}_2^m$ for some $m \leq n$. We shall use the following notation for X a subset of a ring R, and r an element of R:

$$Xr := \{xr | x \in X\}.$$

Algorithm 2 Compute the primitive idempotents of $R = Re_{2,1}$

1: $X_0 := \{1\}$
2: **for** $i = 1$ to d **do**
3: $X_i := X_{i-1}g_i \bigcup X_{i-1}(1 - g_i)$
4: **end for**
5: **return** $X_d \setminus \{0\}$

Notice that for each i, X_i consists of elements which are mutually orthogonal, so that it has no more than $m+1$ elements, thus the algorithm runs in time polynomial in n. Moreover, we claim that $X_d \setminus \{0\}$ is the set of all primitive idempotents of R. Notice that each $f \in X_d \setminus \{0\}$ is a product of d elements of R, where the i^{th} factor is either equal to g_i or to $1 - g_i$. This means that either $g_i f = 0$ or $(1 - g_i)f = 0 \Leftrightarrow g_i f = f$, for all $i \in \overline{1,d}$. Therefore $Gf = \{0, f\}$ generates Rf, so that $Rf = Gf$ as sets, which is possible only if f is primitive. An easy induction argument show that $\sum_{f \in X_i} f = 1$, $\forall i \in \overline{0,d}$, so that $\sum_{f \in X_d \setminus \{0\}} = 1$. In particular, we obtain that $X_d \setminus \{0\}$ is the set of all primitive idempotents of R.

• The case $p \geq 3$. Since $R \simeq \mathbb{F}_p^m$ for some $m < n$, then any nonzero $x \in R$ can be written uniquely as $x = \sum_{f \in F(x)} x_f \cdot f$, $x_f \in \mathbb{F}_p$, where $F(x)$ is a finite set of mutually orthogonal idempotents satisfying $\sum_{f \in F(x)} f = 1$ and $x_f \neq x_g$, for all $f \neq g$ with $f, g \in F(x)$. We shall call this expression the *step representation* of x. In the

first part of this subsection we show that there exists a probabilistic polynomial time algorithm that computes (with overwhelming probability) the step representation of any nonzero element of R. Then, we find the primitive idempotents by applying this subroutine to the generating set.

Consider the following algorithm with input $x \in R$ and $r \in \{0, 1, ..., p-1\}$:

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

1: Compute $x(r) := \frac{(x-r\cdot 1_R)^{p-1}+(x-r\cdot 1_R)^{\frac{p-1}{2}}}{2}$
2: **return:** $\{x(r), 1-x(r)\}$

The algorithm $\mathcal{A}(x, r)$ returns a set consisting of two idempotents with sum equal to 1. Indeed, if $x = \sum_{f\in F(x)} x_f \cdot f$ is the step representation of f, then

$$x(r) = \sum_{f\in F(x)} \frac{(x_f - r)^{p-1} + (x_f - r)^{\frac{p-1}{2}}}{2} \cdot f,$$

and $\frac{(x_f-r)^{p-1}+(x_f-r)^{\frac{p-1}{2}}}{2} \in \{0, 1\}$, for all $f \in F(x)$. If x is an integer multiple of the unit, i.e. $F(x) = \{1_R\}$, then the algorithm always returns the set $\{0_R, 1_R\}$. Otherwise, the following proposition predicts that for any two distinct idempotents $f, g \in F(x)$, the algorithm returns two idempotents that separate them (i.e. either $Supp\{f\} \subseteq Supp\{x(r)\}, Supp\{g\} \cap Supp\{x(r)\} = \emptyset$ or vice versa) for at least one third of all possible values of r.

Proposition 6. Let $x \in R$ be such that $x \neq a \cdot 1_R$ for any $a \in \mathbb{F}_p$, and let $f, g \in F(x)$ be two distinct idempotents. Then, the probability that the algorithm $\mathcal{A}(x, r)$ returns a set consisting of two idempotents that separate f and g is at least $\frac{1}{2} - \frac{1}{2p} \geq \frac{1}{3}$, when r is chosen uniformly at random from the set $\{0, 1, ..., p-1\}$.

Proof. Let us first observe that we may assume $F(x) = \{f, g\}$, i.e. $x = x_f \cdot f + x_g \cdot g$. If $\chi((x_f - r)(x_g - r)) = -1$ then it is easy to see that the algorithm returns two idempotents that separate f and g (here $\chi(a) = a^{\frac{p-1}{2}}$, $a \in \mathbb{F}_p$ is the Legendre symbol). To count how many r's have this property, we count first how many r's satisfy $\chi((x_f - r)(x_g - r)) = 1$. This is equal to:

$$\begin{aligned}
\sum_{r\neq x_f, x_g} \frac{1+\chi((x_f-r)(x_g-r))}{2} &= \frac{p-2}{2} + \frac{1}{2}\sum_{r\neq x_f, x_g} \chi((x_f-r)(x_g-r)) \\
&= \frac{p-2}{2} + \frac{1}{2}\sum_{r\neq x_f, x_g} \chi\left(\frac{x_f-r}{x_g-r}\right) \\
&= \frac{p-2}{2} + \frac{1}{2}\sum_{s\neq 0,1} \chi(s) = \frac{p-3}{2},
\end{aligned}$$

where the second to the last equality follows from the fact that the map $r \mapsto \frac{x_f-r}{x_g-r}$ is a bijection from $\mathbb{F}_p \setminus \{x_f, x_g\}$ to $\mathbb{F}_p \setminus \{0, 1\}$, and the last equality is a consequence of $\sum_{s\in\mathbb{F}_p^\times} \chi(s) = 0$, for any nontrivial character. Thus, the required probability is at least $\frac{1}{p}\left(p - 2 - \frac{p-3}{2}\right) = \frac{1}{2} - \frac{1}{2p}$. □

The following probabilistic algorithm, which uses $\mathcal{A}(x,r)$ as a subroutine, outputs $F(x)$ with overwhelming probability, for any input $x \in R$.

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

$X_0 := \{1\}$
    for $i = 1$ to M **do**
        Pick r uniformly at random from $\{0, 1, ..., p-1\}$ and run $\mathcal{A}(x,r)$
        $X_i := \bigcup_{y \in \mathcal{A}(x,r)} X_{i-1}y$
    end for
return: $X_M \setminus \{0\}$

We have the following estimation:

Proposition 7. For every $x \in R \setminus \{0\}$, the algorithm $\mathfrak{Equal}(x, M)$ outputs $F(x)$ with probability at least $1 - \binom{n}{2}(\frac{2}{3})^M$.

Proof. According to Proposition 6, the probability that there exist two distinct idempotents of $F(x)$ that are not separated in any of the M runs of $\mathcal{A}(x,r)$ is at most $\binom{|F(x)|}{2}(\frac{2}{3})^M$. Since the number of idempotents in $F(x)$ is less than or equal to the number of primitive idempotents, and that is at most n, the result follows. □

Remark 7. Notice that if one chooses $M = \lceil \frac{2n+100}{\log_2 3-1} \rceil$, then the probability that the algorithm $\mathfrak{Equal}(x)$ outputs $F(x)$ is at least

$$1 - \binom{n}{2}\left(\frac{2}{3}\right)^M \geq 1 - \frac{\binom{n}{2}}{2^{2n+100}} \geq 1 - \frac{1}{2^{n+100}} \geq \max\left(1 - \frac{1}{2^{100}}, 1 - \frac{1}{2^n}\right).$$

In other words, the algorithm outputs $F(x)$ with overwhelming probability for every n, and, in addition, the probability is exponentially close to 1 as $n \to \infty$. Of course, if p is small (i.e. p is polynomial in n) we can modify $\mathfrak{Equal}(x)$ by running $\mathcal{A}(x,r)$ for all $r \in \overline{0, p-1}$. In that case the output is $F(x)$ and the algorithm becomes a deterministic polynomial time algorithm.

Now, we are proceeding similarly to the case $p = 2$ to compute the primitive idempotents:

Algorithm 5 Compute the primitive idempotents of $R = Re_{p,1}$

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

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

By Proposition 7, in the above algorithm the equalities $\bar{F}(g_i) = F(g_i)$ hold for all $i \in \overline{1,d}$ with probability at least $1 - d\binom{n}{2}(\frac{2}{3})^M$. In this case, the output of the algorithm is the set of all primitive idempotents. Indeed, since $g_i \cdot f \in \mathbb{F}_p f$,

$\forall i \in \overline{1,d}$, $\forall f \in F(g_i)$, we get that $g_i \cdot f \in \mathbb{F}_p f$, $\forall i \in \overline{1,d}$, $\forall f \in X_d \setminus \{0\}$. Suppose that there exist an idempotent $f \in X_d \setminus \{0\}$ that is not primitive, then we can write f as a sum of primitive idempotents $f = e_1 + ... + e_k$, $k \geq 2$. Since $\{g_1 f, ..., g_d f\}$ is generating Rf, we get that $Rf \simeq \mathbb{F}_p f$, which is a contradiction because $\mathbb{F}_p f$ is not isomorphic to $\prod_{i=1}^{k} \mathbb{F}_p e_i$. We proved that $X_d \setminus \{0\}$ consists only of primitive idempotents. Multiplying the equalities $\sum_{f \in F(g_i)} f = 1$ for all $i \in \overline{1,d}$, we get that

$$\sum_{f \in X_d \setminus \{0\}} f = 1,$$

so that $X_d \setminus \{0\}$ is the set of all primitive idempotents (see Remark 1). As before, if, for example, one chooses $M = \lceil \frac{2n+d+100}{\log_2 3 - 1} \rceil$ then the algorithm outputs the set of all primitive idempotents with probability at least $\max\left(1 - \frac{1}{2^{100}}, 1 - \frac{1}{2^n}\right)$ and runs in time polynomial in (n, d).

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

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

The following algorithm takes as input a nonzero element x and outputs a set of mutually orthogonal idempotents, such that, for each one of them, the primitive components of x that correspond to the primitive idempotents in its support are Galois conjugates.

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

1: $F := \{1\}$
2: **for** $i = 1$ to k
3: Compute $u_j(x) := s_j(x, x^p, \dots x^{p^{k-1}})$
4: $E_j := \mathfrak{Equal}(u_j(x))$
5: $F = E_j \cdot F$
6: **end for**
7: **return:** $F \setminus \{0\}$

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

Algorithm 7 $\mathfrak{Conj}\, G$

1: $F := \{1\}$
2: **for** $i = 1$ to d
3: $X_i := \mathfrak{Conj}(g_i)$
5: $F = X_i \cdot F$
6: **end for**
7: **return:** $F \setminus \{0\}$

If f is in the output of $\mathfrak{Conj}\, G$ then the primitive components of $g_i f$ are Galois conjugates, for all $i \in \overline{1,d}$. Therefore, by Lemma 3, if we replace R by Rf and G by Gf, we reduce to the case in which the primitive components of any element of the generating set are Galois conjugates. For the rest of this section we shall assume that this is the case.

Before we give the algorithm for this final case, we need to discuss and recall the theoretical background needed. To this end, it is convenient to introduce the set $\mathrm{GalConj}(R)$ consisting of all elements of R for which their primitive components are Galois conjugates. We have the following characterization of this set:

Lemma 5. *An element $x \in R$ is in GalConj(R) if and only if $\mathbb{F}_p[x]$ is a field.*

Proof. Observe that the restriction $\pi_{1_{|_{\mathbb{F}_p[x]}}} : \mathbb{F}_p[x] \to \mathbb{F}_{p^k}$ is injective when x is in $\mathrm{GalConj}(R)$, so that $\mathbb{F}_p[x]$ is a field. Conversely, let $x_i := \pi_i(x)$ and $x_j := \pi_j(x)$ 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 wouldn'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 conjugates. □

For any $x \in \mathrm{GalConj}(R)$, we define the degree of x by:

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

It is clear that $k(x) = \min\{j \in \mathbb{N} | x^{p^j} = x\}$, and if R is an (n,d)-BBR then $k(x) \leq n$.

Lemma 6. *Let $x, y \in$ GalConj(R) with $\gcd(k(x), k(y)) = 1$, then $\mathbb{F}_p[x,y]$ is a field.*

Proof. For any $i \in \{2, ..., n\}$, there exist integers u_i, v_i such that $x_i = x_1^{p^{u_i}}$, and $y_i = y_1^{p^{v_i}}$ (as before $x_j = \pi_j(x)$, $y_j = \pi_j(y)$, $\forall j$). 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 to $\mathbb{F}_p[x,y]$ is injective, hence $\mathbb{F}_p[x,y]$ is a field. □

The rest of this section is heavily influenced by the results of [26], 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 exists $\bar{g} \in \mathrm{GalConj}(R)$ with $k(\bar{g}) = k$. The following algorithm is called **combine_gen** in [26] , we shall make it suitable for our situation:

Algorithm 8: combine_gen(a, b)

1: Let $a, b \in \mathrm{GalConj}(R)$
2: Find $k_a | k(a)$ and $k_b | k(b)$ such that:

$$\gcd(k_a, k_b) = 1, \mathrm{lcm}(k_a, k_b) = \mathrm{lcm}(k(a), k(b))$$

3: Find $a' \in \mathbb{F}_p[a], b' \in \mathbb{F}_p[b]$ such that $k(a') = k_a$, $k(b') = k_b$.
4: **return:** $a' + b'$

This algorithm takes as input two elements $a, b \in \mathrm{GalConj}(R)$ and returns an element $x \in \mathrm{GalConj}(R)$ with $k(x) = \mathrm{lcm}(k(a), k(b))$. Step 2 and Step 3 are explained in [26], and the arguments also work in our case because $\mathbb{F}_p[a], \mathbb{F}_p[b]$ are fields. Notice that $a', b' \in \mathrm{GalConj}(R)$, and since $\gcd(k_a, k_b) = 1$ we get that $\mathbb{F}_p[a', b']$ is a field, by Lemma 6. Since $\mathbb{F}_p[a' + b']$ is a subfield of $\mathbb{F}_p[a', b']$, by Lemma 5, we get that $a' + b' \in \mathrm{GalConj}(R)$. 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 $k(a' + b') = k(a') \cdot k(b') = \mathrm{lcm}(k(a), k(b))$.

The purpose of the following algorithm is to find an element $\bar{g} \in \mathrm{GalConj}(R)$ with $\mathbb{F}_p[\bar{g}] \simeq \mathbb{F}_{p^k}$.

Algorithm 9: Computing $\bar{g}$

1: Let $\{g_1, ..., g_d\}$ be a generating set for R.
2: Set $\bar{g} := g_1$
3: **for** $i = 2$ to d **do**
4: $\bar{g} :=$ **combine_gen**$(\bar{g}, g_i)$
5: **end for**
6: **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 $\mathbb{F}_{p^k}$ 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. $\mathbb{F}_p[\bar{g}] \simeq \mathbb{F}_{p^k}$.

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 $\mathrm{tr}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(\bar{g}^i h_j) = \delta_{i+1,j}$, where $\mathrm{tr}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(x) := x + x^p + ... + x^{p^{k-1}}$, for any $x \in R$ (see [26] for the calculation of the dual basis inside the black-box field $\mathbb{F}_p[\bar{g}]$).

Now, we use this dual basis to compute the primitive idempotents of $R = Re_{p,k}$.

Algorithm 10 Compute the primitive idempotents of $Re_{p,k}, k \geq 2$

1: **for** $i = 1$ to d **do**
2: Compute $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j)$, $\forall j$
3: Let $X_i := \prod_j \mathfrak{Equal}(\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(g_i h_j))$
4: **end for**
5: **return:** $F := \left(\prod_i X_i\right) \setminus \{0\}$

Proposition 8. The above algorithm takes as input and (n,d)-BBR $R=(Re_{p,k})^{red}$ with generating set consisting only of elements from $GalConj(R)$ and outputs the set of all primitive idempotents of R. Moreover, the algorithm runs in time polynomial in (n,d).

Proof. By Proposition 7, we have that $\sum_{f\in F} f = 1$, so that it remains to prove that each $f \in F$ is primitive; equivalently, the ring Rf has no zero divisors. For any $f \in F$, we claim that $g_i f \in \mathbb{F}_p[\bar{g}]f$ for all $i \in \overline{1,d}$. Assuming the claim, then the ring generated by $\{g_i f | i \in \overline{1,d}\}$ is a subring of the field $\mathbb{F}_p[\bar{g}]f$, 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.

To prove the claim, notice first that by Proposition 7 we have:

$$\mathrm{tr}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(g_i h_j) f \in \mathbb{F}_p f, \forall i,j.$$

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

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

If e is any primitive idempotent that occurs in the sum decomposition of f then $\mathrm{tr}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(x_i h_j)e = \mathrm{tr}_{\mathbb{F}_{p^k}/\mathbb{F}_p}(x_i e \cdot h_j e) = 0$. This, together with the fact that $\{h_j e | j \in \overline{1,d}\}$ is a basis of $Re \simeq \mathbb{F}_{p^k}$, implies that $x_i e = 0$; hence $x_i = 0, \forall i$. We get that:

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

which ends the argument. □

6. Applications

6.1. **The Representation Problem.** In this subsection, we extend the results of [26] to the case of a reduced p-power BBR. More precisely, the authors of [26] study the Representation Problem (see the next definition) for a black-box field, and we consider the same problem for a BBR that is isomorphic to a finite product of finite fields, all of a fixed characteristic p. As in [26], we have the following:

Definition 4. (Representation Problem) Consider an (n,d)-BBR R and a generating set $G = \{g_1, ..., g_d\}$ of it. For any $x \in R$, finding a polynomial $P(X_1, ..., X_d) \in \mathbb{Z}[X_1, ..., X_d]_+$ such that $x = P(g_1, ..., g_d)$ is called the *representation problem for the black-box ring R.*

We state the following extension of Theorem 1 from [26]:

Theorem 11. *The representation problem for a reduced p-power (n,d)-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 (classically) the primitive idempotents of the reduced p-power BBR in terms of the generating set, more precisely as polynomials in the elements of the generating set. Hence, we reduce the representation problem for a reduced p-power BBR to the representation problem for each of its local Artinian components. Now, since each local Artinian component is a finite field of characteristic p, the theorem follows from Maurer and Raub's result, which asserts that the representation problem for a black-box field of characteristic p is efficiently reducible to the representation problem for $\mathbb{F}_p$. □

Since the representation problem for $\mathbb{F}_p$ with p small (i.e. p is polynomial in n) is clearly solvable, we have the following:

Corollary 5. If R is a reduced p-power (n,d)-BBR and p is small then the representation problem for R is efficiently solvable.

Remark 8. We refer the reader to [26] for the connection between the representation problem and the extraction and isomorphism problems for black-box fields. As in [26], our result shows that the extraction and isomorphism problems for a reduced p-power BBR are efficiently reducible to the representation problem for $\mathbb{F}_p$.

6.2. **Homomorphic Encryption.**

6.2.1. *Definitions.* The homomorphic encryption schemes in their generality were treated by different authors and many treaties. We refer to [22] for a comprehensive treatment of the subject and also to [3] for a treatment of their security behavior. Let us define ring homomorphic encryption schemes and explore their properties. Since a ring homomorphic encryption scheme is a certain type of a homomorphic encryption scheme, we introduce first this concept. In what follows, λ will indicate the security parameter.

Definition 5. A *public key encryption scheme* consists of three PPT algorithms

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

as follows:

- Key Generation. The algorithm $(pk, sk) \leftarrow \mathbf{KeyGen}(1^\lambda)$ takes a unary representation of the security parameter and outputs a public encryption key pk and a secret decryption key sk.
- Encryption. The algorithm $c \leftarrow \mathbf{Enc}(pk, m)$ takes the public key pk and a single message m and outputs a ciphertext c.
- Decryption. The algorithm $m^\star \leftarrow \mathbf{Dec}(sk, c)$ takes the secret key sk and a ciphertext c and outputs a message $m^\star$.

A public key encryption scheme is assumed to be *correct*, i.e. it satisfies the following property:
Correct Decryption: The scheme $\mathcal{E}$ is *correct* if for all $m \in \mathcal{M}$ and keys (sk, pk) in the support of $\mathbf{KeyGen}(1^\lambda)$,

$$\Pr[\mathbf{Dec}(sk, \mathbf{Enc}(pk, m)) = m] = 1,$$

where the probability is over the randomness of **Enc**.

A *public-key homomorphic encryption scheme* is a public-key encryption scheme with an additional PPT evaluation algorithm **Eval**, such that **KeyGen** outputs an additional evaluation key evk besides sk and pk. More precisely, we have:

- Homomorphic Evaluation. The algorithm $c_f \leftarrow \mathbf{Eval}(evk, f, c_1, ..., c_\ell)$ takes the evaluation key evk, a circuit $f : \mathcal{M}^\ell \to \mathcal{M}$ ($\mathcal{M}$ is the message space) from a set of circuits $\mathcal{C}$, and a set of ℓ ciphertexts $c_1, ..., c_\ell$, and outputs a ciphertext.

A public-key homomorphic encryption scheme is assumed to satisfy the following properties:

Correct Evaluation: The scheme $\mathcal{E}$ *correctly evaluates* all circuits in $\mathcal{C}$ if for all keys (sk, pk, evk) in the support of $\mathbf{KeyGen}(1^\lambda)$, for all circuits $f : \mathcal{M}^\ell \to \mathcal{M}$, $f \in \mathcal{C}$, and for all $m_i \in \mathcal{M}$, $1 \leq i \leq \ell$, it holds that

$$\Pr[\mathbf{Dec}(sk, \mathbf{Eval}(evk, f, (c_i)_{i=1}^\ell)) = f((m_i)_{i=1}^\ell)] = 1,$$

where $c_i \leftarrow \mathbf{Enc}(pk, m_i)$, $\forall i \in \overline{1, \ell}$, and the probability is over the randomness of **Enc** and **Eval**.

Compactness: The scheme $\mathcal{E}$ is *compact*, if there exists a polynomial $s = s(\lambda)$ such that the output length of **Eval** is at most s bits long, regardless of f or the number of inputs.

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

Definition 6. An *arithmetic circuit* over a ring R is defined similarly to a standard boolean circuit, except that each wire carries an element of R and each gate can perform an addition or multiplication operation over R (for a more formal definition see Definition 4.1. in [1]).

In this work we will consider only the following type of homomorphic encryption schemes:

Definition 7. A *ring homomorphic encryption (RHE) scheme* is an encryption scheme such that the message and the ciphertext spaces are finite rings, the addition and multiplication on these spaces can be performed by polynomial time algorithms, and the decryption algorithm is a homomorphism of rings for any secret key outputted by the key generation algorithm.

More precisely, in Definition 7 we assume the existence of two representations: $R_\lambda \overset{\imath_R}{\hookrightarrow} \{0,1\}^{n_R(\lambda)}$ and $S_\lambda \overset{\imath_S}{\hookrightarrow} \{0,1\}^{n_S(\lambda)}$, where $n_R(\lambda), n_S(\lambda)$ are polynomials in the security parameter λ (here R_λ and S_λ are the ciphertext space and the message space), such that $\mathbf{Dec}_\lambda(sk, \cdot) : \imath_R(R_\lambda) \to \imath_S(S_\lambda)$ is a deterministic polynomial time algorithm, and $\mathbf{Enc}_\lambda(pk, \cdot) : \imath_S(S_\lambda) \rightsquigarrow \imath_R(R_\lambda)$ is a probabilistic polynomial time algorithm. Notice that since **Dec** is a homomorphism of rings a RHE correctly decrypts any arithmetic circuit, so that a RHE is a homomorphic encryption scheme for the set of all arithmetic circuits (for compactness, observe that the output of **Eval** is always at most $n_R(\lambda)$ bit long). We note here that the evaluation key of an RHE scheme may consists of the necessary parameters needed to define the two operations on the ciphertext space.

The main motivation for the study of RHE schemes comes from the fact that if the plaintext space of a RHE scheme is a quasi-unital ring (see section 3), then

the RHE scheme gives rise to a FHE scheme. By Theorem 3 and Proposition 1 the plaintext space S_λ contains a non-zero idempotent, say e, so that one can construct an $\mathbb{F}_2$-structure inside S_λ. Indeed, the set $\{0, e\}$ together with addition $x \oplus y = 2(x+y) - (x+y)^2$ and usual multiplication from S is a ring isomorphic to $\mathbb{F}_2$. To show that the encryption scheme with message space $\{0, e\}$ and with encryption and decryption enherited from the RHE scheme is a fully homomorphic encryption scheme, one defines the **Eval** algorithm as follows: replace any gate of a boolean circuit with the corresponding small degree polynomial (i.e. the XOR gate is replaced by $\oplus$ and the AND gate by the usual multiplication) and use the operations on the ciphertext space. The fact that **Dec** is a homomorphism of rings shows that the scheme correctly evaluates any boolean circuit.

We briefly recall the security notion that we consider in this paper, that is indistinguishability under chosen-ciphertext attack (IND-CCA^1) for public key encryption schemes (see [25]). To define it we introduce first the following two-phase experiment in which $\mathcal{A}$ is a polynomial time adversary.

$\mathrm{Expr}^{\text{IND-CCA}^1}$:

- Phase One: Generate the keys $(pk, sk, evk) \leftarrow \mathbf{KeyGen}(1^\lambda)$. Give $\mathcal{A}$ access to a decryption oracle and run $\mathcal{A}$ on input (pk, evk). The adversary $\mathcal{A}$ proposes two messages m_0 and m_1.
- Phase Two: Choose at random a bit i, and compute $c \leftarrow \mathbf{Enc}(pk, m_i)$. 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.

Let us point out that the above experiment is relative to a fixed encryption scheme. The experiment can be run on encryption schemes which are not homomorphic by letting the evaluation key to be the empty set.

Definition 8. An encryption scheme $\mathcal{E}$ is IND-CCA^1 secure if for any polynomial time adversary $\mathcal{A}$, *the advantage of* $\mathcal{A}$ satisfies:

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

We extend the above definition so that we include adversaries who have access to quantum computation only in Phase One of the IND-CCA^1 experiment. This naturally leads to the notion of *quantum-classical* IND-CCA^1 secure scheme. From a practical point of view this notion seems reasonable, given the nowadays restrictive access to quantum computing facilities.

In what follows, we shall assume that the ciphertext space of a ring homomorphic encryption scheme is an (n, d)-BBR (where n and d are polynomials in the security parameter). In particular, the attacks that we construct on RHE schemes do not depend on the knowledge of the addition or multiplication algorithms of the ciphertext space.

6.2.2. *IND-CCA^1-attack on ring homomorphic encryption schemes over quasi-unital rings.* The aim of this subsection is to present the following cryptanalysis result:

Theorem 12. *If the plaintext space of a ring homomorphic encryption scheme is a quasi-unital ring, then the scheme is not quantum-classical 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. By this assumption and the fact that the decryption map is a surjective homomorphism, we get that R is a quasi-unital BBR. In Phase One, the adversary uses the algorithms from Section 5 to find the primitive idempotents of R (notice that the time complexity of this computation is polynomial in the security parameter). Then, it starts decrypting the primitive idempotents using the decryption oracle, until he finds a nonzero decryption, say $f \overset{\text{Dec}}{\longmapsto} m$. Now, the adversary $\mathcal{A}$ proposes the messages m and 0, which ends Phase One of the IND-CCA^1 experiment.

If $c \leftarrow \mathbf{Enc}(m)$ is any encryption of m, then

$$\mathbf{Dec}(cf) = \mathbf{Dec}(c) \cdot \mathbf{Dec}(f) = m \cdot m = m,$$

so that $\mathbf{Dec}(\mathbf{e}(cf)) = m$. This, together with the fact that $\mathbf{e}(cf)$ is either equal to f or to 0 (because f is a primitive idempotent), yields that $\mathbf{e}(cf) = f$. The argument also shows that if c is an encryption of 0 then $\mathbf{e}(cf) = 0$.

Consequently, in Phase Two of the IND-CCA^1 experiment, the adversary computes $\mathbf{e}(cf)$ and outputs m if $\mathbf{e}(cf) = f$ and 0 otherwise. Notice that since Rf is a p-power oracle ring, by Proposition 3, $\mathbf{e}(cf)$ is computed classically in polynomial time. It is clear that the adversary decrypts correctly with probability equal to 1 any given ciphertext.

□

6.2.3. *Decrypting ciphertexts in RHE schemes over reduced rings of smooth characteristic.* In this subsection, we investigate a plaintext-recovery attack on ring homomorphic encryption schemes, whose plaintext spaces are reduced rings of smooth characteristic. This means that the plaintext space is a product of fields, such that each field that occurs in the product has small (that is polynomial in the security parameter) characteristic. More precisely, we shall investigate the following type of plaintext-recovery two-phase attack (called *quantum-classical plaintext-recovery attack*).

- In the first phase, the adversary receives the public key and access to a decryption oracle. In this phase, the adversary is allowed to do computation using classical and quantum PPT algorithms.
- In the second phase, after receiving a ciphertext from the challenger, the adversary is allowed to use only classical PPT algorithms in order to find the decryption of the ciphertext.

We say that a quantum-classical plaintext-recovery attack is *successful* if it decrypts correctly with probability equal to 1.

Theorem 13. *Let $\mathcal{E}$ be a ring homomorphic encryption scheme whose plaintext space S is a reduced ring of smooth characteristic, then there is a successful quantum-classical plaintext-recovery attack.*

Proof. Let R be the ciphertext space of $\mathcal{E}$. We have the following commutative diagram:

$$\begin{array}{ccccc} R & \xrightarrow{\cdot \bar{e}_R} & \bar{R} & \longrightarrow & Re_j \xrightarrow{\rho_j \circ \pi_j} R_j^{red} \\ \Big\downarrow{\scriptstyle \mathbf{Dec}} & & \Big\downarrow{\scriptstyle \mathbf{Dec}} & & \Big\downarrow{\scriptstyle \mathbf{D}_j} \swarrow{\scriptstyle \Psi_j} \\ S & \xrightarrow{=} & S & \longrightarrow & Sf_j \end{array}$$

where Re_j is a local Artinian component of R, and $f_j = \mathbf{Dec}(e_j)$. Also, D_j is the restriction of the decryption map to Re_j, and R_j^{red} is the associated BBR structure of the residue field of Re_j (cf. Corollary 3). We recall that each primitive idempotent of S gives rise to a unique primitive idempotent of R which decrypts to it (cf. Corollary 1), so that the map $\mathbf{D}_j : Re_j \to Sf_j$ in the diagram refers to such a pair. Since Sf_j is a field, $\mathbf{D}_j$ factors over the projection map $\rho_j \circ \pi_j : Re_j \to R_j^{red}$ (see the proof of Corollary 2), so that we get the map Ψ_j in the diagram. Notice that Ψ_j is an isomorphism of fields. Since injectivity is clear, it remains to prove surjectivity. Let $s \in S$ and $r \leftarrow \mathbf{Enc}(s)$, then $\mathbf{Dec}(r) = s$ so that $\mathbf{D}_j(re_j) = sf_j$; therefore $\mathbf{D}_j$ is surjective, and the same holds for Ψ_j.

Now we describe the plaintext-recovery attack. First of all, since the ciphertext space is an (n, d)-BBR a finite set G of generators for R is given. The adversary $\mathcal{A}$ uses the decryption oracle to decrypt the elements of G (we point out that this is the only time when the decryption oracle is needed). Then $\mathcal{A}$ computes the primitive idempotents of R, and decrypts each one of them using its polynomial expression in terms of the generating set. Now, the adversary records the pairs $\{(e_j, f_j = \mathbf{Dec}(e_j))|j \in J\}$, where e_j, f_j are both primitive idempotents of R and S, respectively (some of the primitive idempotents of R do not appear in this set because they decrypt to 0). Let us note that the map Ψ_j is efficiently computable. Indeed, the set Ge_j generates Re_j, so that $\rho_j \circ \pi_j(Ge_j)$ is a generating set for R_j^{red}, and we know how Ψ_j maps the elements of this set, because we know the values of $\mathbf{D}_j$ on Ge_j. Now, the result of Maurer and Raub ([26], Theorem 1) shows how to represent each element of R_j^{red} in terms of this generating set, therefore we know how to compute the map Ψ_j (for more details see Section 3.3 of *loc.cit.*). Finally, the adversary uses the following formula satisfied by the decryption map:

$$\mathbf{Dec}(c) = \sum_{j \in J} \Psi_j(ce_j), \forall c \in R$$

□

Remark 9.

• In general, under the assumptions of the last theorem, the above argument shows that decryption map may be computed correctly when the representation problem is solvable for any prime divisor of the characteristic of the plaintext space.

• Under the assumptions of the last theorem, if R and S are unital with known characteristics, then the above plaintext-recovery attack can be performed using only classical algorithms.

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

References

[1] Applebaum, B., Ishai, Y., Kushilevitz, E.: How to Garble Arithmetic Circuits, SIAM Journal of Computing, Volume 43, Issue 2, 2014, pp. 905 - 929.

[2] Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C. A., Strand, M.: A guide to fully homomorphic encryption, IACR Cryptology ePrint Archive, 2015, 1192, https://eprint.iacr.org/2015/1192.pdf.

[3] Armknecht, F., Katzenbeisser, S., Peter, A.: Group Homomorphic Encryption: Characterizations, Impossibility Results, and Applications, Designs, Codes and Cryptography, Volume 67, Number 2, 2013, pp. 209 - 232.
[4] Aggarwal, D., Maurer, U.: Breaking RSA Generically Is Equivalent to Factoring, In Advances in Cryptology - EUROCRYPT 2009, Lecture Notes in Computer Science, Volume 5479, pp. 36 - 53.
[5] Atiyah, M. F., Macdonald, I. G.: Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.
[6] Babai, L., Szemerédi, E.: On the complexity of matrix group problems I, In Proc. 25th IEEE Symposium on the Foundation of Computer Science, 1984, pp. 229 - 240.
[7] Barcau, M., Paşol, V.: Ring Homomorphic Encryption Schemes, IACR Cryptology ePrint Archive, 2018, 583, https://eprint.iacr.org/2018/583.pdf.
[8] Boneh, D., Lipton, R. J.: Algorithms for Black-Box Fields and their Application to Cryptography, Advances in Cryptology - CRYPTO 96, Lecture Notes in Computer Science, Volume 1109, pp. 283 - 297.
[9] Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE, In IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Rafail Ostrovsky editor, pp. 97 - 106.
[10] Brakerski, Z.: Fully homomorphic encryption without modulus switching from classical GapSVP, In Advances in Cryptology - CRYPTO 2012, Lecture Notes in Computer Science, Volume 7417, pp. 868 - 886.
[11] 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.
[12] Childs, A.M., Ivanyos, G.: Quantum computation of discrete logarithms in semigroups, Journal of Mathematical Cryptology, Volume 8, Number 4, 2014, pp. 405 - 416.
[13] Childs, A.M., van Dam, W.: Quantum algorithms for algebraic problems, Reviews of Modern Physics, Volume 82, Issue 1, 2010, pp. 1 - 52.
[14] Coron, J-S., Mandal, A., Naccache, D., Tibouchi, M.: Fully homomorphic encryption over the integers with shorter public keys, Advances in Cryptology - CRYPTO 2011, Lecture Notes in Computer Science, Volume 6841, pp. 487 - 504.
[15] van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully homomorphic encryption over the integers, In Advances in Cryptology - EUROCRYPT 2010, Lecture Notes in Computer Science, Volume 6110, pp. 24 - 43.
[16] Doröz, Y., Hoffstein, J., Pipher, J., Silverman, J.H., Sunar, B., Whyte, W., Zhang, Z.: Fully Homomorphic Encryption from the Finite Field Isomorphism Problem, IACR Cryptology ePrint Archive, 2017, 548, https://eprint.iacr.org/2017/548.
[17] Damgard,I., Koprowski, M.: Generic Lower Bounds for Root Extraction and Signature Schemes in General Groups, Advances in Cryptology - EUROCRYPT 2002, Lecture Notes in Computer Science, Volume 2332, pp. 256 - 271.
[18] Gentry, C.: A fully homomorphic encryption scheme, PhD thesis, Stanford University, 2009.
[19] 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.
[20] 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, Rafail Ostrovsky editor, pp. 107 - 109.
[21] 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, Volume 8042, 2013, pp. 75 - 92.
[22] Halevi, S.: Homomorphic Encryption, In Tutorials on the Foundations of Cryptography, part of the Information Security and Cryptography book series, Springer Verlag 2017, pp. 219 - 276.
[23] Jager, T., Schwenk, J.: On the Analysis of Cryptographic Assumptions in the Generic Ring Model, Advances in Cryptology - ASIACRYPT 2009, Lecture Notes in Computer Science, Volume 5912, pp. 399 - 416.
[24] Lidl, R., Niederreiter, H.: Finite Fields, Encyclopedia of Mathematics and its Applications, Volume 20, Cambridge University Press, 2nd edition, 1997.

[25] Loftus, J., May, A., Smart, N.P., Vercauteren, F.: On CCA-Secure Somewhat Homomorphic Encryption, In: Miri, A., Vaudenay, S. (eds) Selected Areas in Cryptography, SAC 2011, Lecture Notes in Computer Science, Volume 7118, pp. 55 - 72.
[26] 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, Volume 4833, pp. 427 - 443.
[27] Rivest, R., Adleman, L., Dertouzos, M.: On data banks and privacy homomorphisms, In Foundations of Secure Computation, Academic Press, 1978, pp. 169 - 177.
[28] 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.
[29] 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.
[30] Shoup, V.: Lower Bounds for Discrete Logarithms and Related Problems, Proceedings of EUROCRYPT 1997, Lecture Notes in Computer Science, Volume 1233, pp. 256 - 266.
[31] Smart, N., Vercauteren, F. Fully homomorphic encryption with relatively small key and ciphertext sizes, Public Key Cryptography – PKC 2010, Lecture Notes in Computer Science, Volume 6056, pp. 420 - 443.

certSIGN - Research and Development, Bucharest, Romania and Simion Stoilow Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, 014700 Bucharest, Romania

Email address: mugurel.barcaul@imar.ro

certSIGN - Research and Development, Bucharest, Romania and Simion Stoilow Institute of Mathematics of the Romanian Academy, P.O. Box 1-764, 014700 Bucharest, Romania

Email address: vicentiu.pasol@imar.ro