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. We also prove that the reduction of a black-box ring is also a black-box ring. As a first application, we extend the work of Maurer and Raub [24] 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 key-recovery attack based on representation problem in black-box prime fields. In particular, if the ciphertext space has smooth characteristic, the key-recovery attack is effectively computable in the generic ring model.

generic ring model and black-box rings and primitive idempotents and quantum computing and homomorphic encryption schemes

1. Introduction

Many researcher have used for more than 20 years algorithms in generic models as a tool in proving reductions for hardness assumptions. These assumptions are the foundation for the security of public key schemes which enable such schemes to exist in the first place. 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 [28]. Therein and since then, a variety of cryptographic problems were proven to be computationally intractable in the generic group model, most notably the Discrete Logarithm problem, the computational Diffie-Hellman problem [28], as well as the RSA problem over groups of hidden order [16].

Similarly, generic ring models are used to analyze the hardness of computational problems defined over rings. For example, it is proved in [22] 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 [3] 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 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, but in fact, 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 such a ring is isomorphic to a product of local Artinian rings. We shall provide an algorithm that computes explicitly this decomposition. Furthermore, each of the local Artinian factors is endowed with a BBR structure. Explicitly, we prove the following:

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

(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 5.5). We proceed by reducing to the case where R is a product of isomorphic finite fields (Proposition 4). Furthermore, we prove first our result in the prime field case using an algorithm which produces with positive probability perpendicular 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 shall say a few words about fully homomorphic encryption (FHE). This is one of the most important problems of modern cryptography, which asserts the existence of an encryption scheme that allows evaluation of arbitrarily complex programs on encrypted data, while the data remains encrypted. The problem was suggested by Rivest, Adleman and Dertouzos in [25], where it was called "privacy homomorphism".

Any efficient FHE would have a large number of practical applications such as: medical applications, financial privacy, consumer privacy in advertising, forensic image recognition, etc. (see [1]).

In [17], C. Gentry came up with the first construction of such a scheme based on ideal lattices. Gentry's approach goes as follows: first, he constructs a somewhat homomorphic encryption scheme which is an encryption scheme that supports evaluating low-degree polynomials on the encrypted data; next, he "squashes" the

decryption procedure so that it can be expressed as a low-degree polynomial which is supported by the scheme; and finally, he develops a bootstrapping technique which allows one to obtain a fully homomorphic scheme. The first generation of fully homomorphic encryption schemes ([18], [14], [29], [13], [19]) was constructed following Gentry's recipe.

A second generation of encryption schemes started in [8], where fully homomorphic encryption was established in a simpler way, based on the learning with errors assumption; the scheme was then improved in [10]. Currently, perhaps the simplest FHE scheme based on the learning with errors assumption is by Brakerski [9] who builded on Regev's public key encryption scheme [26]. The most recent achievement in this direction was obtained in [20], where a significant FHE scheme was introduced claiming three important properties: simpler, faster, and attribute-based FHE.

Another very recent approach aiming for producing FHE was presented in [15], where the authors based their construction on the finite field isomorphism problem. All these schemes are based on the method of constructing a noisy version of the ciphertext (the noise is added to guarantee the security of the cryptosystem). 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. 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. It is worth mentioning that in the 1996 paper of Boneh and Lipton [7], 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 homomorphic one-way permutation. It is shown in [24] 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 $\mathbb{F}_p$ is to find a polynomial 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 [24]). 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 an 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 key-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 [24] 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 general quasi-unital rings and, in the case of ring homomorphic encryption schemes over a reduced ring, we present a key-recovery attack in the generic ring model.

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 bellow, 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 bellow). 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. No information about its algebraic structure can be deduced from this representation.

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

By a finite generating set of a (nonunital) ring R, we understand a finite subset $\{g_1, g_2, ..., g_d\}$ of R such that any element of the ring can be written in the form $P(g_1, g_2, ..., g_d)$, where $P(X_1, ..., X_d) \in \mathbb{Z}[X_1, ..., X_d]_+$, i.e. $P(0, ..., 0) = 0$. If R is a unital ring, then the unity itself can be written as a polynomial with integer coefficients in the set of generators, however this expression is not known a priori.

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. Even if we assume that one can check whether $x \in I$ for $x \in R$, there is no obvious way to give a representation for $R^{red} := R/Nil(R)$ as in the above definition. The solution to this problem will be a key ingredient in our practical applications:

Theorem 2. *If R is a BBR, then R^{red} is also a BBR.*

We postpone the proof of this theorem until Section 5.4. The difficulty of the proof of this theorem is to realize R^{red} as an oracle ring, and an explicit realization of 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 accomplish our goal 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.** If R is a commutative ring, then $x \in R$ is called *idempotent* if $x^2 = x$. Moreover, $x \in R$ is called a *primitive idempotent* if x is an 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 $e_2 = 0$.

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 we denote by $E(R)$ the idempotent semigroup associated to the semigroup $(R, \cdot)$. If we define addition in $E(R)$ by: $e \oplus e' = e + e' - 2ee'$, $\forall e, e' \in E(R)$, then this becomes a ring of characteristic 2. We shall refer to this ring $(E(R), \oplus, \cdot)$ as being the *idempotent ring* of R, or the idempotent $\mathbb{F}_2$-algebra of R. It is shown in [5], 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, then $x^{k \cdot p(x)}$ is an idempotent for a sufficiently large k. In fact, this is the unique idempotent belonging to the sequence. We shall denote by $\mathbf{e}(x)$ this idempotent.

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

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

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

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

Remark 1. 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 [4]) 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 $\mathbb{F}_2^n$. Notice that if R is a ring with unity, then $1 = e_1 + ... + e_n$, where $e_1, ..., e_n$ are the primitive idempotents of R. Therefore, the map $R \to \prod Re_i$, $x \mapsto (xe_1, ..., xe_n)$ is an isomorphism, so that the rings R_i are in fact isomorphic to the rings Re_i. In particular, the number of local Artinian rings that appear in the decomposition of R is equal to the number of its primitive idempotents (for more details see [5]).

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

Lemma 1. *Let R be a commutative BBR and e an explicit idempotent. Then, the ring $S := Re$ is a BBR.*

Proof. The ring S inherits the oracle ring structure from R. If $G = \{g_1, ..., g_d\}$ is a set of generators of R, then $Ge := \{g_1e, ..., g_de\}$ is a generating set of S. □

Lemma 2. *Let $R_1, ..., R_n$ be a finite set of BBRs, where n is polynomial in λ. Then, the product $\prod_{i=1}^n R_i$ is a 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 have the following explicit version 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. See the proof of the next remark. □

Remark 2. 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.

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

Remark 3. The unicity of the decomposition in Theorem 3 may be shown as follows: 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:

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 $y^{q^n} = x$ for any n with $\mathfrak{m}^n = (0)$.*

Proof. Since R is complete in the $\mathfrak{m}-$adic topology, the first part of the theorem is just an application of Hensel's lemma: let $y_i := y^{q^i}$, $\forall i \geq 1$, then we have $y_1 \equiv y \bmod \mathfrak{m}$, 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 $y_n = y_{n-1}$ for any n such that $\mathfrak{m}^n = (0)$. Denoting by x this stationary value, we get that $x^q = x$ and $x \equiv y \mod \mathfrak{m}$. □

Remark 4. Under the conditions of theorem 6, we have: $\mathbf{e}(y) = y^{q^n(q-1)} \in \{0, 1\}$.

We have the following useful consequence of Theorem 6 :

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

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

Definition 2. 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 BBR whose Artinian local rings have residue fields isomorphic to a fixed finite field $\mathbb{F}_q$, then R^{red} is a BBR.

Proof. As in Corollary 2, let $S = \{x \in R | x^q = x\}$. Let $R = \prod_i R_i$, where $(R_i, \mathfrak{m}_i)$ are its local Artinian components. As above, on S we define the addition $x +_S y = (x + y)^{q^n}$, where n is the nilpotency index of the ideal $\prod_i \mathfrak{m}_i$ (one can take $n = \lfloor \log_q |R| \rfloor$, see the proof of Proposition 3). Then $(S, +_S, \cdot)$ becomes a ring isomorphic to R^{red}, where $\cdot$ is the multiplication inherited from R. In particular, we get that R^{red} is an oracle ring. Notice that, if $G = \{g_1, ..., g_m\}$ is a set of generators for R, then $G^{red} := \{g_1^{q^n}, ..., g_m^{q^n}\}$ is a set of generators for S, consequently R^{red} is a 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 bellow. 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 [11](see also [12], [5]), and is an adaptation of Shor's algorithm(see [27]).

Proposition 2. Given an oracle semigroup G and an element $g \in G$, there is an efficient polynomial time quantum algorithm that computes the period $p(g)$.

Remark 5. The authors of [11] 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 polynomial time quantum algorithm that computes the map $\mathbf{e} : R \to E(R)$, when R is a commutative oracle ring.

Proof. Choose an integer k such that $kp(g) > |R|$, and compute $\mathbf{e}(g) = g^{kp(g)}$. □

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

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

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 $R = R_1 \times ... \times R_n$, where each R_i is a local finite ring with maximal ideal $\mathfrak{m}_i$, and residue field $R_i/\mathfrak{m}_i \simeq \mathbb{F}_{p^{k_i}}$. We may suppose that $\mathfrak{m}_i^{N_i} = (0)$, and that N_i is the least positive integer with this property. If $y = (y_1, ..., y_n)$, the, by Remark 4, we obtain that

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

Since $R_i \supset \mathfrak{m}_i \supset \mathfrak{m}_i^2 \supset ... \supset \mathfrak{m}_i^{N_i} = (0)$ and each $\mathfrak{m}_i^j/\mathfrak{m}_i^{j+1}$ is a (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 $k_i \leq \log_p |R|$ 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. *Let R be a commutative black box ring. There exists a polynomial-time quantum algorithm that computes all its primitive idempotents.*

In other words, we show an explicit way of computing the decomposition $R = \prod_i Re_i \times N_R$, where e_i are the primitive idempotents of R. Our strategy runs as follows:

(1) We first compute the unital part of a ring R by computing $\bar{e}_R$.
(2) For a unital ring R, we compute its p-power parts by computing the idempotents e_p for which Re_p is the maximal p-power subring of R.
(3) For a unital p-power ring R, we compute, for each positive integer k, an idempotent $e_{p,k}$ such that $Re_{p,k}$ is the maximal subring of R whose residue fields are all isomorphic to $\mathbb{F}_{p^k}$.
(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 computing is used only to determine each e_p (with p prime) and N_R. After this step, only classical computing will be used.

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

Theorem 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 $R_k = Re_k$, $k \in \overline{1,n}$ 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. □

According to Lemma 1, $\bar{R}$ is a BBR. Since $\bar{R}$ is a unital ring, we may assume from now on that R is a unital commutative BBR.

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

Theorem 9. *Let R be a unital commutative oracle ring with an explicit representation of its unit. Then, there exists a polynomial time quantum algorithm that determines for all primes p an idempotent e_p, such that $R = \prod_p Re_p$, and Re_p is a p-power ring. Moreover, if R is a BBR then each ring Re_p is a unital p-power BBR.*

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

(1) Use Shor's quantum algorithm to compute the characteristic of R, i.e. the minimal positive integer N such that $N \cdot 1_R = 0$ (see Proposition 2).
(2) Use Shor's quantum factorization algorithm to compute the prime factorization of $N = \prod_p p^{\alpha_p}$ (see [27]).
(3) Use Euclidean algorithm to compute integers u_p such that $\frac{N}{p^{\alpha_p}} \mid u_p$ and $\sum_p u_p = 1$.
(4) Set $e_p := u_p \cdot 1_R$.

It is easy to check that, indeed, e_p are orthogonal idempotents with sum 1_R. Moreover, the ring R_p has all its residual characteristics equal to p. By Lemma 1, R_p inherits a BBR structure from R. □

5.3. **Computing the subrings $R_{p,k}$.** The aim of this subsection is to show how to compute the idempotents $e_{p,k}$, which determine the rings $R_{p,k} := Re_{p,k}$. As explained in Remark 6, from now on all proposed algorithms are classical. We have the following result:

Theorem 10. *Let R be a unital p-power BBR, and let $G = \{g_1, \ldots, g_d\} \subseteq R$ be a set of generators for the ring R. There exists an explicit polynomial time algorithm that determines for all positive integers k an idempotent $e_{p,k}$ such that $R = \prod_k Re_{p,k}$, and $R_{p,k} = Re_{p,k}$ is a p-power BBR with all its residue fields isomorphic to $\mathbb{F}_{p^k}$.*

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

Algorithm 1 Compute $e_{p,k}$

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

10: **end while**
11: **return** $e_{p,k}, k \geq 1$

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 $m \geq k+1$. Consider a primitive idempotent e_j. If $\mathbf{e}(g_i - g_i^p) \cdot e_j = e_j$ for some i, then $R_j/\mathfrak{m}_j \not\simeq \mathbb{F}_p$. Indeed, otherwise $g_i e_j \equiv (g_i e_j)^p = g_i^p e_j \mod \mathfrak{m}_j$, so that

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

which is a contradiction. Hence $\bar{e}_{p,1}$ is a sum of primitive idempotents with corresponding residue fields non-isomorphic to $\mathbb{F}_p$. Moreover, $\bar{e}_{p,1}$ is the sum of all primitive idempotents with corresponding residue fields non-isomorphic to $\mathbb{F}_p$. Let e_j be a primitive idempotent with corresponding residue field non-isomorphic to $\mathbb{F}_p$. Since $\{g_1 e_j \mod \mathfrak{m}_j, ..., g_d e_j \mod \mathfrak{m}_j\}$ generates $R_j/\mathfrak{m}_j$ and $R_j/\mathfrak{m}_j$ is non-isomorphic to $\mathbb{F}_p$, there exist an i such that $g_i e_j - (g_i e_j)^p \notin \mathfrak{m}_j$, therefore $\mathbf{e}(g_i - g_i^p) e_j = e_j$, which proves our claim. A similar argument works inductively for any k, because multiplication by $\bar{e}_{p,k-1}$ restricts to the Artinian local components of R with corresponding residue fields of size at least p^k. □

5.4. **Proof of Theorem 2.** Let R be a commutative BBR. Since $R^{red} \simeq \bar{R}^{red}$, and by Lemma 1 $\bar{R} = R\bar{e}$ is a BBR, we may assume that R is a unital BBR. By Theorems 9 and 10, $R = \prod_p \prod_k R_{p,k}$, and each $R_{p,k}$ is a BBR (Lemma 1). According to Lemma 2, since $R^{red} \simeq \prod_p \prod_k R_{p,k}^{red}$, it is enough to prove the theorem when $R = R_{p,k}$, i.e. R is a unital commutative BBR with all residue fields isomorphic to $\mathbb{F}_q = \mathbb{F}_{p^k}$. But this is exactly the statement of Corollary 3.

5.5. **Computing the primitive idempotents of $R_{\mathbf{p,k}}$.** The purpose of this section is to show how to compute the primitive idempotents of a ring R with isomorphic residue fields $\mathbb{F}_q = \mathbb{F}_{p^k}$. According to the next proposition we can work with R^{red}, instead of R. Indeed, we have the following result:

Proposition 4. Let R be a p-power ring BBR whose Artinian local rings have residue fields isomorphic to a fixed finite field $\mathbb{F}_q$, and let S be the R^{red}'s BBR structure as in Corollary 3, then R and S have the same primitive idempotents.

Proof. Let e be a primitive idempotent of R, then e is also an idempotent in S. Suppose that $e = e_1 +_S e_2$ with $e_1 \cdot e_2 = 0$. We obtain that $e = (e_1 + e_2)^{q^n} = e_1 + e_2$, which yields that either $e_1 = 0$ or $e_2 = 0$. The other way around, let $e = e_1 + e_2$ with $e_1 \cdot e_2 = 0$; then $e = e_1 + e_2 = e_1 +_S e_2$, therefore either $e_1 = 0$ or $e_2 = 0$. □

Remark 7. The above proposition shows that $E(S) = E(R)$ as rings. This fact can be checked directly by computation, which in turn proves that R and S have the same primitive idempotents.

Throughout the rest of this section we assume in addition that R is a reduced ring, i.e. R is a product of isomorphic finite fields.

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

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

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

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

1: $X_0 := \{1\}$
2: **for** $i = 1$ to d **do**
3: $X_i := g_i X_{i-1} \bigcup (1 - g_i) X_{i-1}$
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 $n + 1$ elements, i.e. at most a polynomial (in the security parameter) number of elements. Moreover, we claim that $X_d \setminus \{0\} := \{f_1, \ldots f_r\}$ is the set of all primitive idempotents of R. Notice that each f_j is a product of elements of R, each factor being equal to either g_i or $1 - g_i$, for some i. This means that either $g_i f_j = 0$ or $(1 - g_i) f_j = 0 \Leftrightarrow g_i f_j = f_j$, for all $i \in \overline{1, d}$, therefore G generates only $\mathbb{F}_2 \cdot f_j$ inside Rf_j, which is possible only if f_j is primitive.

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

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:** $\{x(r), 1 - x(r)\} \setminus \{0\}$

Notice that if $a \in \mathbb{F}_p$, then $\chi(a) := a^{\frac{p-1}{2}}$ is the Legendre symbol, i.e. the primitive quadratic character on $\mathbb{F}_p$. The algorithm $\mathcal{A}(x, r)$ returns either $\{1\}$ or a set consisting of two idempotents whose sum is equal to 1. If x is an integer multiple of the unit then the algorithm always returns $\{1\}$. Otherwise, the following result predicts that for at least one third of the values of r the algorithm returns a set consisting of two idempotents with sum equal to 1.

Proposition 5. Let $x \in R$ be such that $x \neq a \cdot 1_R$ for any $a \in \mathbb{F}_p$. Then, the probability that the algorithm $\mathcal{A}(x, r)$ returns a set consisting of two idempotents is at least $\frac{1}{2} - \frac{1}{2p} \geq \frac{1}{3}$, when r is uniformly chosen from the set $\{0, 1, ..., p - 1\}$.

Proof. Let us compute the probability for $n = 2$, i.e. $x = ae_1 + be_2$ with $a \neq b \in \mathbb{F}_p$. The algorithm returns two values at least when $\chi((a - r)(b - r)) = -1$. To count how many r's have this property, we count first how many r's satisfy

$\chi((a-r)(b-r))=1$. This is equivalent to finding the number of solutions of the equation $y^2=(x-a)(x-b)$ over $\mathbb{F}_p$ with $y\neq 0$, which is given by

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

where the second to the last equality follows from the fact that the map $x\mapsto\frac{x-a}{x-b}$ is a bijection from $\mathbb{F}_p\setminus\{a,b\}$ to $\mathbb{F}_p\setminus\{0,1\}$, and the last equality is a consequence of $\sum_{x\in\mathbb{F}_p^\times}\chi(x)=0$, for any nontrivial character. Thus, the required probability is greater than or equal to $\frac{1}{p}\left(p-2-\frac{p-3}{2}\right)=\frac{1}{2}-\frac{1}{2p}$.
In general, for $n\geq 2$, by our assumption there exists primitive idempotents $e_i\neq e_j$ such that $x(e_i+e_j)=ae_i+be_j$ with $a\neq b\in\mathbb{F}_p$. Since

$$\mathcal{A}(x(e_i+e_j),r)(e_i+e_j)=\mathcal{A}(x,r)(e_i+e_j),$$

if the algorithm returns two values for $x(e_i+e_j)$ then it does the same for x. This proves that the probability for $n\geq 2$ is at least as large as the probability for $n=2$. □

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

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

1: $X_0:=\{1\}$
2: **for** $i=1$ to $\Theta(\lambda)$ **do**
3: Pick r uniformly at random from $\{0,1,...,p-1\}$ and run $\mathcal{A}(x,r)$
4: $X_i:=\bigcup_{y\in\mathcal{A}(x,r)}yX_{i-1}$
5: **end for**
6: **return:** $F(x):=X_{\Theta(\lambda)}\setminus\{0\}$

Proposition 6. Let $x\in R\setminus\{0\}$. Then, the algorithm $\mathfrak{Equal}(x)$ returns, with probability greater than $1-(\frac{2}{3})^{\Theta(\lambda)}$, an orthogonal set $F:=F(x)$ consisting of non-zero idempotents with sum equal to 1, such that $x=\sum_{f\in F}x_f\cdot f$, $x_f\in\mathbb{F}_p$.

Proof. According to Proposition 5, the probability that $xf\in\mathbb{F}_pf$, $\forall f\in F$ is at least $1-(\frac{2}{3})^{\Theta(\lambda)}$. Since $1=\sum_{f\in F}f$, we get

$$x=x\cdot 1=\sum_{f\in F}xf,$$

which proves the required equality. □

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

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

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

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

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

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

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

The following algorithm takes as input a non-zero element x and outputs a set of orthogonal idempotents, such that for each one of them, the corresponding primitive components 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:** $F \setminus \{0\}$

The above algorithm togheter with Lemma 1 allow us to reduce to the case in which the primitive components of any element of the generating set are Galois conjugates. In other words, for each $f \in \mathfrak{Conj}G$ we replace R by Rf, and G by fG. It is convenient to introduce the set 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 3. *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 $\pi_1 : \mathbb{F}_p[x] \to \mathbb{F}_q$ is injective when x is in GalConj(R), so that $\mathbb{F}_p[x]$ is a field. Conversely, let x_i and x_j be two distinct primitive components of $x \in R$, and let $Q(X)$ be the minimal polynomial of x_i over $\mathbb{F}_p$. We get that the i^{th} and j^{th} components of $Q(x) \in R$ are 0 and $Q(x_j)$, respectively. If $Q(x_j) \neq 0$, then $Q(x)$ were a zero divisor in R, so that it 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 $x \in \text{GalConj}(R)$ we define the size:

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

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

Lemma 4. *Let $x, y \in$ GalConj(R) with $\gcd(k(x), k(y)) = 1$, then $\mathbb{F}_p[x, y]$ is a field.*

Proof. Let $i \in \{2, ..., n\}$, then $x_i = x_1^{p^{u_i}}$, and $y_i = y_1^{p^{v_i}}$, for some integers u_i, v_i. Since $(k(x), k(y)) = 1$, by the Chinese Remainder Theorem, there exist an integer N_i such that $N_i \equiv u_i \pmod{k(x)}$, and $N_i \equiv v_i \pmod{k(y)}$, so that $x_i = x_1^{p^{N_i}}$, and $y_i = y_1^{p^{N_i}}$. Consequently, the restriction of π_1 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 [24], where R is just a finite field. The main arguments are there, we just verified that they can be extended to our case. First of all we show that there exist $\bar{g} \in \text{GalConj}(R)$ with $k(\bar{g}) = k$. The following algorithm is called **combine_gen** in [24] , we shall make it suitable for our situation:

Algorithm 8: combine_gen(a, b)

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

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

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 $a, b \in \text{GalConj}(R)$ and returns an element $x \in \text{GalConj}(R)$ with $k(x) = \text{lcm}(k(a), k(b))$. Step 2 and Step 3 are explained in [24], and the arguments also work in our case because $\mathbb{F}_p[a], \mathbb{F}_p[b]$ are fields. Notice that $a', b' \in \text{GalConj}(R)$, and since $\gcd(k_a, k_b) = 1$ we get that $\mathbb{F}_p[a', b']$ is a field, by Lemma 4. Since $\mathbb{F}_p[a' + b']$ is a subfield of $\mathbb{F}_p[a', b']$, by Lemma 3, we get that $a' + b' \in \text{GalConj}(R)$. Obviously $\mathbb{F}_p[a', a' + b'] = \mathbb{F}_p[a' + b', b'] = \mathbb{F}_p[a', b']$ so that:

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

We get that $k(a' + b') = k(a') \cdot k(b') = \text{lcm}(k(a), k(b))$.

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

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

By the well-known dual basis theorem [23], there exist an $\mathbb{F}_p$-basis $h_1, ..., h_k$ of $\mathbb{F}_p[\bar{g}]$ such that $\text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(\bar{g}^i h_j) = \delta_{i+1,j}$, where $\text{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) := x + x^p + ... + x^{p^{k-1}}$, for any $x \in R$ (see [24] 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 $R = R_{p,k}$.

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

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

Proposition 7. The above algorithm outputs the set of all primitive idempotents of $R = R_{p,k}$.

Proof. By Proposition 6, 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 6 we have:

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

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

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

If e is any primitive idempotent that occurs in the sum decomposition of f then $\mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_i h_j)e = \mathrm{tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_i e \cdot h_j e) = 0$. This, togheter with the fact that $\{h_j e | j \in \overline{1,d}\}$ is a basis of $Re \simeq \mathbb{F}_q$, 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 [24] to the case of a reduced p-power BBR. More precisely, the authors of [24] 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 [24], we have the following:

Definition 3. (Representation Problem) Consider a black-box ring R and a generating set $G = \{g_1, ..., g_d\}$ of it. If $x \in R$, then 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 [24]:

Theorem 11. *The representation problem for a reduced p-power BBR is efficiently reducible to the representation problem for $\mathbb{F}_p$.*

Proof. The results of sections 5.3 and 5.5 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 $\mathbb{F}_p$. □

Consequently, we have the following:

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

Remark 8. We refer the reader to [24] for the connection between the representation problem and the extraction and isomorphism problems for black-box fields. As in [24], 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 [21] for a comprehensive treatment of the subject and also to [2] for a treatment of their security behavior. Let us define ring homomorphic encryption schemes and explore their properties. We use λ to indicate the security parameter. Since a ring homomorphic encryption scheme is a certain type of homomorphic encryption scheme, we introduce first this concept.

Definition 4. A *homomorphic (public-key) encryption scheme*

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

is a quadruple of PPT algorithms as follows:

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

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

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

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

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

Definition 5. A homomorphic scheme **HE** is *fully homomorphic* (**FHE**) if it is compact and homomorphic for the class of all circuits.

Remark 9. If one weakens the compactness condition, one can construct such schemes as in [6].

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

Definition 6. A *ring homomorphic encryption scheme* (**RHE**) is a **HE** scheme given by a family (indexed by λ) of quadruples $(R_\lambda, S_\lambda, \mathbf{Enc}_\lambda, \mathbf{Dec}_\lambda)$, consisting of finite rings R_λ, S_λ, homomorphism of rings $\mathbf{Dec}_\lambda(sk, \cdot) : R_\lambda \to S_\lambda$, and PPT algorithm $R_\lambda \ni c \leftarrow \mathbf{Enc}_\lambda(pk, m)$, where $m \in S_\lambda$, such that the following conditions hold:

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

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

Remark 10. If the plaintext space is a quasi-unital ring (see section 3), then a ring homomorphic encryption scheme is a fully homomorphic encryption scheme. Indeed, by Theorem 3 and Proposition 1 the plaintext space S_λ contains a non-zero idempotent, so that one can construct an $\mathbb{F}_2$-structure inside S_λ. To show that such a ring homomorphic encryption scheme is a fully homomorphic encryption scheme, one replaces any gate of a boolean circuit with the corresponding small degree polynomial and use the homomorphicity of the decryption map.

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

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

Definition 7. A scheme **HE** is IND-CCA^1 secure if for any polynomial time adversary $\mathcal{A}$, *the advantage of* $\mathcal{A}$ satisfies:

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

We shall also say that a scheme is *quantum-classical* IND-CCA^1 secure if the adversary $\mathcal{A}$ is allowed to use classical and quantum algorithms in the first phase, whereas

in the second phase the adversary is allowed to use only classical algorithms. In the same manner, one can define quantum-quantum IND-CCA^1 security etc..

In what follows, we shall assume that the ciphertext space of a ring homomorphic encryption scheme is a black-box ring.

6.2.2. *IND-CCA$^1-$attack on ring homomorphic encryption schemes over quasi-unital rings.* The aim of this subsection is to present one of our main cryptanalysis results:

Theorem 12. *If the plaintext space of a ring homomorphic encryption scheme is a quasi-unital ring, then the scheme is not IND-CCA$^1-$secure.*

Proof. Suppose that R and S are the ciphertext space, and respectively the plaintext space of a ring homomorphic encryption schemes, and that S is a quasi-unital ring. By this assumption and the fact that the decryption map is a surjective homomorphism, we get that R is a quasi-unital BBR. The adversary uses the algorithms from Section 5 to find the primitive idempotents of R. Then, he 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 for the IND-CCA^1 experiment.

Since any ciphertext $c \leftarrow \text{Enc}(m)$ satisfies $\mathbf{e}(cf) = f$, and any $c \leftarrow \text{Enc}(0)$ satisfies $\mathbf{e}(cf) = 0$, the adversary will decrypt c by computing $\mathbf{e}(cf)$; more precisely, if he gets f then he outputs m, and if he gets 0 then he outputs 0. It is clear now, that the adversary decrypts correctly with probability equal to 1 any given ciphertext.

□

Remark 11. As we mentioned in the Introduction, the adversay uses quantum computations only in the process of finding the primitive idempotents of the ciphertext space, which is part of the first phase of the experiment. In the second phase, the adversay uses only classical algorithms to decrypt the ciphertexts. Thus, we have constructed a quantum-classical IND-CCA^1 attack. Finally, notice that one needs to assume that the plaintext is quasi-unital, because otherwise all primitive idempotents of R decrypt to 0.

6.2.3. *Key-recovery attack for ring homomorphic encryption schemes over reduced rings of smooth characteristic.* We investigate in this subsection the security of ring homomorphic encryption schemes with plaintext space a reduced ring 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 characteristic.

For such schemes we construct an efficient key-recovery attack, by which we understand a polynomial time algorithm that decrypts correctly any ciphertext.

Theorem 13. *Let $(R, S, \text{Dec}, \text{Enc})$ be a ring homomorphic encryption scheme whose plaintext space S is a reduced ring of smooth characteristic. Given access to a decryption oracle, there exist an efficient (quantum) key-recovery attack.*

Proof. We consider the following commutative diagram:

$$\begin{array}{ccccccc} R & \xrightarrow{\cdot\bar{e}_R} & \bar{R} & \longrightarrow & Re_j & \longrightarrow & R_j^{red} \\ \Big\downarrow{\scriptstyle \text{Dec}} & & \Big\downarrow{\scriptstyle \text{Dec}} & & \Big\downarrow{\scriptstyle \text{D}_\text{j}} & \swarrow{\scriptstyle \Psi_j} & \\ S & \xrightarrow{=} & S & \longrightarrow & Sf_j & & \end{array}$$

where Re_j is a local Artinian component of R, and $f_j = \mathrm{Dec}(e_j)$. 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 $D_j : Re_j \to Sf_j$ in the diagram refers to such a pair. Since Sf_j is a field, D_j factors over the projection map $Re_j \to R_j^{red}$, 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 $r \leftarrow \mathrm{Enc}(s)$, then $\mathrm{Dec}(r) = s$ so that $D_j(re_j) = sf_j$; therefore D_j is surjective, and the same holds for Ψ_j.

Now we describe the key-recovery attack. First of all, use the decryption oracle to decrypt the elements of the generating set G of R. We point out that this is the only time when we need the decryption oracle. Compute the primitive idempotents of R, and decrypt each one of them using its polynomial expression in terms of the generating set. Record the pairs $\{(e_j, f_j = \mathrm{Dec}(e_j))|j \in J\}$, 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). Notice that the map Ψ_j is efficiently computable. Indeed, the set Ge_j, which generates Re_j, gives rise to a generating set of R_j^{red}, and we know where Ψ_j maps this set, because we know the values of D_j on Ge_j. Now, the result of Maurer and Raub ([24], 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, we compute the decryption map using the formula

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

□

Remark 12.
• 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.
• Still under the assumptions of the last theorem, if R and S are unital with known characteristic, then the key recovery attack can be performed using only classical computations.
• Since our strategy for the key-recovery attack uses in an essential way the computation of idempotents, we cannot deduce any information about the nilpotent part. This is why we had to assume in the last theorem that the plaintext is a reduced ring.

References

[1] 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.
[2] 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.
[3] 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.

[4] Atiyah, M. F., Macdonald, I. G.: Introduction to commutative algebra, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.
[5] Barcau, M., Paşol, V.: Ring Homomorphic Encryption Schemes, IACR Cryptology ePrint Archive, 2018, 583, https://eprint.iacr.org/2018/583.pdf.
[6] Barcau, M., Paşol, V.: Bounded Fully Homomorphic Encryption from Monoid Algebras, IACR Cryptology ePrint Archive, 2018, 584, https://eprint.iacr.org/2018/584.pdf.
[7] 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.
[8] 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.
[9] 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.
[10] 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.
[11] Childs, A.M., Ivanyos, G.: Quantum computation of discrete logarithms in semigroups, Journal of Mathematical Cryptology, Volume 8, Number 4, 2014, pp. 405 - 416.
[12] Childs, A.M., van Dam, W.: Quantum algorithms for algebraic problems, Reviews of Modern Physics, Volume 82, Issue 1, 2010, pp. 1 - 52.
[13] 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.
[14] 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.
[15] 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.
[16] 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.
[17] Gentry, C.: A fully homomorphic encryption scheme, PhD thesis, Stanford University, 2009.
[18] 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.
[19] Gentry, C., Halevi, S.: Fully homomorphic encryption without squashing using depth-3 arithmetic circuits, In IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Rafail Ostrovsky editor, pp. 107 - 109.
[20] Gentry, C., Sahai, A., Waters, B.: Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based, Advances in Cryptology - CRYPTO 2013, Lecture Notes in Computer Science, Volume 8042, 2013, pp. 75 - 92.
[21] 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.
[22] 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.
[23] Lidl, R., Niederreiter, H.: Finite Fields, Encyclopedia of Mathematics and its Applications, Volume 20, Cambridge University Press, 2nd edition, 1997.
[24] 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.
[25] Rivest, R., Adleman, L., Dertouzos, M.: On data banks and privacy homomorphisms, In Foundations of Secure Computation, Academic Press, 1978, pp. 169 - 177.

[26] 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.
[27] 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.
[28] Shoup, V.: Lower Bounds for Discrete Logarithms and Related Problems, Proceedings of EUROCRYPT 1997, Lecture Notes in Computer Science, Volume 1233, pp. 256 - 266.
[29] 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.