Ring Homomorphic Encryption Schemes

Mugurel Barcau Vicenţiu Paşol

Abstract

We analyze the structure of commutative ring homomorphic encryption schemes and show that they are not quantum IND-CCA secure.

1 Introduction

Fully Homomorphic Encryption (FHE) is considered to be the "holy grail" of cryptography. In short, fully homomorphic encryption allows to perform arbitrary computation on encrypted data. The main usability of such a device is to outsource a computation to a remote server without compromising data privacy. In [12], C. Gentry succeeded in describing the first plausible method for constructing fully homomorphic encryption schemes. Gentry's approach consists of several steps: 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 schemes ([13], [11], [24], [10], [15]) constructed following this recipe is based on ideal lattices, which became lately the standard ground for post-quantum cryptology [21]. A second generation of encryption schemes started in [5], where fully homomorphic encryption was established in a simpler way, based on the learning with errors assumption; the scheme was then improved in [7]. Currently, perhaps the simplest FHE scheme based on the learning with errors assumption is by Brakerski [6] who builded on Regev's public key encryption scheme [20]. The most recent achievement in this direction was obtained in [16], where a significant FHE scheme was introduced claiming three important properties: simpler, faster, and attribute-based FHE. Here we emphasize that all these FHE scheme are "noisy" schemes, namely, ciphertexts for these FHE schemes involve "noise" terms to conceal plaintexts. In this respect, an immediate question is whether one can actually construct a noise-free FHE scheme. In such a noise-free FHE scheme, the ciphertext space and the plaintext space should both have ring structures, and the decryption algorithm should be a ring homomorphism, so that one can call such a scheme a ring homomorphic encryption scheme. Moreover, as explained in [14], it is enough to look for a ring homomorphic encryption scheme in which the plaintext is the field with two elements $\mathbf{F}_2$. Let us mention here that a different approach towards achieving noise-free FHE was considered in [19]. Namely, they showed that the NAND operator, which is sufficient for

constructing arbitrary operations on bits, can be realized (in a certain suitable sense) in some non-commutative groups. In this article, we investigate the structure of ring homomorphic encryption schemes, where the ciphertext space is a finite abelian ring R and the plaintext space is the field $\mathbf{F}_2$. To any finite abelian ring R we attach an (idempotent) $\mathbb{F}_2$-algebra $\hat{E}(R)$, such that any homomorphism from R to $\mathbb{F}_2$, in particular the decryption homomorphism, factors over the homomorphism from $\hat{E}(R)$ to $\mathbb{F}_2$. Moreover, since any ring homomorphism from an idempotent $\mathbb{F}_2$-algebra to $\mathbb{F}_2$ is just a projection, one can compute an orthogonal basis of $\hat{E}(R)$ (which is unique up to permutations), and then with overwhelming probability find that projection idempotent, which will play the role of the decryption key. Although we do not give an algorithm to compute such a basis, we show how to (quantum) compute the projection idempotent for any given homomorphism from R to $\mathbb{F}_2$.

We stress out that our method is a quantum attack for the secret key, thus, after the projection element has been found using quantum computations, the decryption is performed classically. If one would allow the decryption algorithm to be performed quantum, then more general results are available. For example, in [1], the authors prove that any (commutative) group encryption scheme is not quantum resistant. However, for decrypting a ciphertext, one has to run every time a quantum algorithm. Apparently, the authors in [1] prove that a group encryption scheme does not meet a stronger security notion, namely IND-CPA. In fact, our proof of IND-CCA insecurity can be modified to their case using precisely the same method (δ-covering subsets). Since this reduction would bring no new insight, we chose to use the case of IND-CCA security, which is equivalent to the uniform sampling assumption in [1].

The plan of the article is as follows: Section 2 is devoted to the study of the structure of finite commutative semigroups while in Section 3 the structure of finite commutative rings is analyzed. In Section 4 we review basic definitions and properties of homomorphic encryption schemes. Section 5 is dedicated to quantum computations on commutative semigroups. In Section 6 we show how to compute the decryption algorithm in ring encryption schemes and prove that any commutative ring homomorphic encryption is not quantum IND-CCA secure. In Section 7 we explicitly compute the structure of monoid algebras in two important cases. We end this article with a brief conclusion section.

2 Finite commutative semigroups

Let $(G, \cdot)$ be a finite commutative semigroup. Two elements $g_1, g_2 \in G$ are called *powerfully equal* if there exist two positive integers m and n such that $g_1^m = g_2^n$. This defines an equivalence relation on G, that will be denoted by $\sim$. If G is a monoid, the equivalence class containing the unit consists of all invertible elements. On the other hand, if we denote by 0 the "absorbing" element of G (if it exists it is unique), defined by $0 \cdot g = 0$, $\forall g \in G$, then the equivalence class containing 0 consists of all nilpotent elements. Since G is finite, any element g satisfies a relation of the form $g^a = g^b$ with $a > b$ positive integers. Such a pair (a, b) is called a *relation pair* for g. Let (a, b) be the minimal (with respect to lexicographic order) relation pair for $g \in G$. Then b is called the *index* and $a - b$ is called the *period* of the element g and they are denoted by $i(g)$, respectively $p(g)$. The subsemigroup of G generated

by g consists of two disjoint parts: the tail part consisting of $\{g, ..., g^{i(g)-1}\}$ and the cyclic part $\{g^{i(g)}, ..., g^{i(g)+p(g)-1}\}$. Notice that the cyclic part is in fact a cyclic group with identity element $g^{kp(g)}$, where $k = \lceil \frac{i(g)}{p(g)} \rceil$ and generator $g^{kp(g)+1}$. The following notion will play an important role in what follows:

Definition 1. A subsemigroup B of G is called a *block* if any two of its elements are powerfully equal.

The equivalence relation on elements induces an equivalence relation on blocks, and we write $A \sim B$ whenever the blocks A and B are equivalent.

Proposition 1. *Let A and B be two blocks in a semigroup G. Then $AB := \{ab | a \in A, b \in B\}$ is again a block. Moreover, $A \sim B$ if and only if $A \cap B \neq \emptyset$, in which case $AB \sim A \sim B$.*

Proof. It is clear that AB is a subsemigroup. To prove that any two elements of AB are powerfully equal it is enough to show $a_1 b \sim a_2 b$, for any $a_1, a_2 \in A$ and any $b \in B$. Let m_1, m_2 two positive integers such that $a_1^{m_1} = a_2^{m_2}$, and consider a positive integer k greater than $\max\{\frac{i(b)}{m_1 p(b)}, \frac{i(b)}{m_2 p(b)}\}$. Then:

$$(a_1 b)^{kp(b)m_1} = a_1^{kp(b)m_1} b^{kp(b)m_1} = a_2^{kp(b)m_2} b^{kp(b)m_1} = a_2^{kp(b)m_2} b^{kp(b)m_2} = (a_2 b)^{kp(b)m_2}$$

The rest of the theorem follows from the definitions.

□

It is useful to take into account the following easy remark:

Remark 2. *Each block contains a unique idempotent element of G. In particular, two equivalent blocks have the idempotent in their intersection.*

It is clear that a class of equivalence in G is a maximal block with respect to inclusion. We have the following:

Proposition 2. *There is a one-to-one correspondence between the idempotents in G and the powerfully equal classes of equivalence. Moreover, the set of all idempotents of G is a subsemigroup $E(G)$ of G, and the operation on $E(G)$ corresponds to the multiplication on blocks.*

Proof. First of all, there is a very easy way to construct the idempotent $e(A)$ corresponding to a block A: pick any element $a \in A$ then $a^{kp(a)}$ is an idempotent where $k = \lceil i(a)/p(a) \rceil$ (in fact one can take any k greater than this value). In a block, the idempotent is unique because any two elements are potentially equal and $e(A)^n = e(A)$ for any positive integer n. Since two nonequivalent classes have empty intersection, they give rise to different idempotents. Now, the proposition follows immediately. □

The above proof shows that for any semigroup G we have a map $e : G \to E(G)$, where $e(g)$ is the unique idempotent in the maximal block of g. As above, $e(a) = a^{kp(a)}$, where $k = \lceil i(a)/p(a) \rceil$. Notice that, since the multiplication on $E(G)$ corresponds to the multiplication on blocks, the map e is a homomorphism of semigroups.

The decomposition of a semigroup in its maximal blocks is considered in the following:

Proposition 3. *Let G be a semigroup. For each $f \in E(G)$, denote by B_f the maximal block in G containing f.*

i) $G = \coprod_{f \in E(G)} B_f$.

ii) For each $f \in E(G)$ let $B_f^0 := \{g \in B_f \mid \exists k \geq 2$ such that $g^k = g\}$. Then B_f^0 is a group with the identity f.

iii) $G^0 := \coprod_{f \in E(G)} B_f^0$ is a subsemigroup of G.

Proof. Assertion i) follows immediately from the previous proposition. Notice that, $g \in B_f$ is in B_f^0 if and only if g is in the cyclic part of some element of B_f. In particular, if $g \in B_f^0$ then the whole cyclic part of g is in B_f^0, therefore the inverse of g is in B_f^0. Now, if $g_1, g_2 \in G$ with $g_1^{k_1} = g_1$ and $g_2^{k_2} = g_2$, then $(g_1 g_2)^{1+(k_1-1)(k_2-1)} = g_1 g_2$. This proves that B_f^0 is a group and G^0 is a subsemigroup of G. □

3 Finite Commutative Rings

In this section we investigate the structure of (non-unital) finite commutative rings and their associated idempotent subrings. As the following proposition shows the structure of the associated idempotent subring is particularly simple. This allows us to fully describe the reduction of any homomorphism of a finite ring to its idempotent subring. In the next section, we shall apply this to the case of commutative ring homomorphic encryption schemes. If R is a ring then we denote by $E(R)$ the idempotent semigroup associated to the semigroup $(R, \cdot)$. It is easy to see that $E(R)$ becomes a ring of characteristic 2 if we define the addition by: $e \oplus e' = e + e' - 2ee'$, $\forall e, e' \in E(R)$. We shall refer to this ring $(E(R), \oplus, \cdot)$ as being the idempotent ring of R, or, as we shall see, as the idempotent $\mathbb{F}_2$-algebra of R.

Proposition 4. *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).

Proof. i) A nonzero element f of $E(R)$ is called *primitive* if it cannot be written as $f = e_1 \oplus e_2$, where e_1, e_2 are *orthogonal* (i.e. $e_1 \cdot e_2 = 0$) nonzero idempotents. Then, any two distinct primitive idempotents are orthogonal. Indeed, Let f, f' be two distinct primitive idempotents. If $f \cdot f' \neq 0$, then since $f = ff' \oplus (f \oplus ff')$ we get $f = ff'$. A similar argument shows that $f' = ff'$, therefore $f = f'$. Primitive elements always exist: assuming the contrary, for any $f \in E(R)$ we obtain an infinite sequence $e_1, \ldots, e_k, \ldots$ of elements such that $f = \sum_{i=k}^{2k} e_i$ and $\{e_i\}_{i=\overline{k,2k}}$ are mutually orthogonal, for any $k \geq 1$. More precisely, if $f = e_k \oplus \ldots \oplus e_{2k}$, since e_k is not primitive, we write $e_k = e_{2k+1} \oplus e_{2k+2}$ with $e_{2k+1} \cdot e_{2k+2} = 0$. Since $e_k e_i = 0$, then for any $k+1 \leq i \leq 2k$ we get that $e_i e_{2k+1} = e_i e_{2k+2}$. Multiplying the last equality by e_{2k+1} yieds $e_i e_{2k+1} = e_i e_{2k+2} = 0$. Since $|E(R)| < +\infty$ we get a contradiction. In fact, the argument shows that any nonzero element of $E(R)$ can be written as a sum of primitive idempotents. Since primitive idempotents are orthogonal, this writing is unique.

Thus, we get a decomposition $E(R) = \bigoplus_e \mathbb{F}_2 e$ where e runs through the finite set of primitive idempotents. Notice that the sum of all primitive idempotents is the unit in $E(R)$, so that $E(R)$ is an $\mathbb{F}_2-$algebra isomorphic to $\mathbb{F}_2^n$, where n is the number of primitive idempotents.

ii) We shall denote from now on by $e_1, ..., e_n$ the primitive elements of $E(R)$; they correspond to the standard basis via the isomorphism $E(R) \simeq \mathbb{F}_2^n$. Since ϕ is a nontrivial homomorphism of rings there exists an $i \in \{1, ..., n\}$ such that $\phi(e_i) = 1$. We prove that $\phi(e_j) = 0, \forall j \neq i$. Supposing that there exist a $j \neq i$ such that $\phi(e_j) = 1$, then $\phi(e_i + e_j) = 0$, and $\phi(e_i) = \phi(e_i(e_i + e_j)) = \phi(e_i)\phi(e_i + e_j) = 0$, which is a contradiction. This shows that ϕ is the projection on the i-th coordinate. □

Remark 3. *If R is a finite ring with unity then it is an Artin ring, and the structure theorem for Artin rings (Theorem 8.7 in [2]) shows that R is isomorphic to a product $R_1 \times ... \times R_n$ of local Artin rings. Notice that a local Artin ring has only two idempotents, these are 0 and 1. The isomorphism $R \simeq R_1 \times ... \times R_n$ gives rise to an isomorphism $E(R) \simeq E(R_1 \times ... \times R_n)$, and since $E(R_1 \times ... \times R_n) = E(R_1) \times ... \times E(R_n) = \mathbb{F}_2 \times ... \times \mathbb{F}_2$, as sets, we obtain*

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

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

As before, if R is a finite ring and $e_1, ..., e_n$ are its primitive idempotents then let $\bar{e} = e_1 \oplus ... \oplus e_n$. Since any two primitive idempotents are orthogonal, $\bar{e} = e_1 + ... + e_n$. We shall denote by $\bar{R}$ the principal ideal of R generated by $\bar{e}$. Notice that $\bar{R}$ is a unital subring of R, its unit being $\bar{e}$. In addition, all idempotents of R are in $\bar{R}$, so that $E(R) = E(\bar{R})$. The following diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & \bar{R} \\ \downarrow{\scriptstyle e_R} & & \downarrow{\scriptstyle e_{\bar{R}}} \\ E(R) & = & E(\bar{R}) \end{array}$$

where e_R and $e_{\bar{R}}$ are the maps that associate to an element its idempotent, and φ is the map $x \mapsto x\bar{e}$. Indeed, we have

$$e_R(x) = e_R(x) \cdot \bar{e} = e_R(x) \cdot e_R(\bar{e}) = e_R(x\bar{e}) = e_{\bar{R}}(\varphi(x)).$$

Suppose now that $\bar{R} \simeq \bar{R}_1 \times ... \times \bar{R}_n$ is the above isomorphism, where $(\bar{R}_i, \mathfrak{m}_i)$ are local Artin rings. We denote by J the set of all indices $j \in \{1, 2, ..., n\}$ for which the residue field $\bar{R}_i/\mathfrak{m}_i$ is isomorphic to $\mathbb{F}_2$. Let $\hat{E}(\bar{R})$ be the $\mathbb{F}_2$-subalgebra of $E(\bar{R})$ generated by all primitive idempotents e_j with $j \in J$. We also let $\hat{E}(R) := \hat{E}(\bar{R})$. Let's consider the following composition of ring homomorphisms:

$$\psi : R \xrightarrow{\varphi} \bar{R} \to \bar{R}_1 \times ... \times \bar{R}_n \to \prod_{i=1}^{n} \bar{R}_i/\mathfrak{m}_i \to \prod_{j\in J} \bar{R}_j/\mathfrak{m}_j \simeq \prod_{j\in J} \mathbb{F}_2$$

where the last map is the obvious projection map. Notice that composing ψ with the inclusion $\iota : \hat{E}(R) \hookrightarrow R$ we get an isomorphism of rings $\psi \circ \iota : \hat{E}(R) \xrightarrow{\sim} \prod_{j\in J} \bar{R}_j/\mathfrak{m}_j$. As we have seen above the map $e_R : R \to E(R)$ is in general a homomorphism of semigroups with respect to multiplication, but is not a homomorphism with respect to addition. On the other hand the composition $\hat{e}_R : R \xrightarrow{e_R} E(R) \to \hat{E}(R)$, where the last map is the obvious projection, is a ring homomorphism. Indeed, it is easy to see that $\hat{e}_R = (\psi \circ \iota)^{-1} \circ \psi$, which proves the claim. For further use, we define $\hat{e} := \sum_{j\in J}^{\oplus} e_j = \sum_{j\in J} e_j$, so that the map $E(R) \to \hat{E}(R)$ is given by $e \mapsto e \cdot \hat{e}$.

Remark 4. *For characteristic* 2 *(nonunital) rings, one has functorial interpretation for the subrings* $E(R)$ *respectively* $\hat{E}(R)$*, an aspect that we will pursue in a forthcoming paper. More precisely,* $E(\cdot)$ *is naturally equivalent to the functor* $Hom(\mathbb{F}_2, \cdot)$ *from the category of rings of characteristic* 2 *to the category of idempotent* $\mathbb{F}_2$*-algebras, while* $\hat{E}(\cdot)$ *is characterized by the universal property that any morphism in* $Hom(R, \mathbb{F}_2)$ *factors through a morphism in* $Hom(\hat{E}(R), \mathbb{F}_2)$*.*

However, in practice, one needs explicit descriptions of these functors. This is the reason we chose not to make categorical analysis in the present work.

4 Homomorphic encryption schemes

The homomorphic encryption schemes in their generality were treated by different authors and many treaties. We refer to [22] for a monograph treatment of the subject and to [3] for a treatment of their security behavior. Let us define ring homomorphic encryption schemes and explore their properties. Throughout this section (and this work) we use λ to indicate the security parameter. Since a ring homomorphic encryption is a certain type of homomorphic encryption scheme, we introduce first these schemes.

A *homomorphic (public-key) encryption scheme* (over $\mathbb{F}_2$)

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

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 bit message $m \in \{0, 1\}$ 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 $m^\star \in \{0, 1\}$.

- **Homomorphic Evaluation.** The algorithm $c_f \leftarrow \mathbf{HE.Eval}_{evk}(f, c_1, ..., c_\ell)$ takes the evaluation key evk, a function $f : \{0,1\}^\ell \to \{0,1\}$ 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 functions $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda\in\mathbb{N}}$, if for any sequence of functions $f_\lambda \in \mathcal{C}_\lambda$ 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, 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 its is compact and homomorphic for the class of all arithmetic circuits over $\mathbb{F}_2$.

In this work we are interested only in the following type of **FHE** scheme:

Definition 6. A *ring homomorphic encryption scheme* is a quadruple $(R_\lambda, \mathbb{F}_2, \mathrm{Enc}_\lambda, \mathrm{Dec}_\lambda)$, consisting of a finite ring R_λ, a homomorphism of rings $\mathrm{Dec}_\lambda : \mathrm{R}_\lambda \to \mathbb{F}_2$, and a PPT algorithm $R_\lambda \ni c \leftarrow \mathrm{Enc}_\lambda(\mathrm{m})$, such that $\mathrm{Dec}_\lambda(\mathrm{c}) = \mathrm{m}$, for any $c \leftarrow \mathrm{Enc}_\lambda(\mathrm{m})$, and the scheme is compact as a homomorphic encryption scheme.

Let us note that compactness is equivalent in this case to the existence of a representation $R_\lambda \overset{\imath}{\hookrightarrow} \{0,1\}^{n(\lambda)}$, where $n(\lambda)$ is a polynomial in λ, such that $\mathrm{Dec}_\lambda : \imath(\mathrm{R}_\lambda) \to \mathbb{F}_2$ is a deterministic polynomial time algorithm, and Enc_λ is a probabilistic polynomial time algorithm, both in the security parameter λ. Since any function $f : \{0,1\}^\ell \to \{0,1\}$ may be represented by a polynomial over $\mathbb{F}_2$, and Dec is a ring homomorphism that correctly decrypts any encryption of a bit message, we see that a ring homomorphic encryption scheme (as a homomorphic encryption scheme) is homomorphic for the class of all arithmetic circuits over $\mathbb{F}_2$.

The only security notion we consider in this paper is quantum indistinguishability under chosen ciphertext attack, quantum IND-CCA for short. To define it we introduce first the following experiment in which $\mathcal{A}$ is a quantum polynomial time adversary.

Experiment quantum IND-CCA
- 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.
- Choose at random a bit message m, and compute $c \leftarrow \mathbf{HE.Enc}_{pk}(m)$. Give c to $\mathcal{A}$ and continue its computation without access to the decryption oracle.
- Let m' be $\mathcal{A}$'s output. Output 1 if $m' = m$ and 0 otherwise.

Definition 7. A scheme **HE** is quantum IND-CCA secure if for any quantum polynomial time adversary $\mathcal{A}$, it holds that

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

5 Quantum Computations on Semigroups

In this section we show that for any semigroup G, the map $G \to E(G)$ can be computed in polynomial time using a quantum algorithm. Since we have no contribution to this result, we have included this section only for completeness. The algorithm we present here was described in [8](see also [9]), and is an adaptation of Shor's algorithm(see [23]).

Proposition 5. *Given a semigroup G and an element $g \in G$, there is an efficient quantum algorithm to determine the period of g.*

Proof. If N is the order of G, then choose a number $M > N^2 + N$ and create the state $\frac{1}{\sqrt{M}} \sum_{j=1}^{M} |j\rangle|g^j\rangle$. Usually, one chooses M to be a power of 2, say $M = 2^m$, because in which case the above state is created as follows: apply the Hadamard transform to each bit in a register of m zeroes to get the superposition $\frac{1}{\sqrt{2^m}} \sum_{j=1}^{2^m} |j\rangle$, and then the algorithm for computing the function $j \mapsto g^j$ is applied in the second (classical) register. Suppose now that we measure the second register, then if we obtain an element g^j in the tail of g (in other words $1 \leq j \leq i-1$), then the first register is left in a computational basis state, which is useless. Fortunately, this happens with probability $\frac{i-1}{M} \leq \frac{N}{M} < \frac{1}{N}$, which is very small($N$ is exponential in the security parameter), so that we repeat the experiment until we obtain an element in the cycle of g, i.e. $j \geq i$. In this case, if we ignore the second register, we get in the first register the superposition $\frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} |x_0 + jp\rangle$, for some $x_0 \in \{i, i+1, ..., i+p-1\}$ and

$$n = \begin{cases} \lfloor \frac{M-i}{p} \rfloor + 1, & \text{if } x_0 \leq M - p\lfloor \frac{M-i}{p} \rfloor \\ \lfloor \frac{M-i}{p} \rfloor, & \text{otherwise.} \end{cases}$$

Apply now the quantum Fourier transform, i.e. the unitary operator defined on the basis state by:

$$|\ell\rangle \mapsto \frac{1}{\sqrt{M}} \sum_{k=1}^{M} \zeta_M^{(\ell-1)(k-1)} |k\rangle,$$

to the above superposition to get:

$$\frac{1}{\sqrt{nM}} \sum_{k=1}^{M} \zeta_M^{(x_0-1)(k-1)} \left(\sum_{j=0}^{n-1} \zeta_M^{jp(k-1)} \right) |k\rangle.$$

After measuring the superposition, the outcome k occurs with probability

$$\mathbf{Pr}(k) = \frac{1}{nM} \left| \sum_{j=0}^{n-1} \zeta_M^{jp(k-1)} \right|^2.$$

If M divides $p(k-1)$ then $\mathbf{Pr}(k) = \frac{n}{M}$, otherwise $\mathbf{Pr}(k) = \dfrac{\sin^2(\frac{\pi(k-1)pn}{M})}{nM \sin^2(\frac{\pi(k-1)p}{M})}$. To show that this probability distribution is strongly peaked around values of k for which $k-1$ is

close to integer multiples of $\frac{M}{p}$, we compute the probability of seeing $k = \lfloor \frac{jM}{p} \rceil + 1$, for some $j \in \mathbb{Z}$. If we write $k = \frac{jM}{p} + \epsilon$, with $|\epsilon| \leq \frac{1}{2}$, then

$$\mathbf{Pr}\left(k = \left\lfloor \frac{jM}{p} \right\rceil + 1\right) = \frac{\sin^2(\pi jn + \frac{\pi \epsilon pn}{M})}{nM \sin^2(\pi j + \frac{\pi \epsilon p}{M})} = \frac{\sin^2(\frac{\pi |\epsilon| pn}{M})}{nM \sin^2(\frac{\pi |\epsilon| p}{M})}.$$

Using the inequalities $\frac{3}{5}x \leq \sin x \leq x$, for all $0 \leq x \leq \frac{\pi}{2} + \frac{\pi}{40}$, and the fact that $\frac{pn}{M} < 1 + \frac{1}{N}$, we obtain:

$$\mathbf{Pr}\left(k = \left\lfloor \frac{jM}{p} \right\rceil + 1\right) \geq \frac{9n}{25M}.$$

Notice that the above bound is very close to $\frac{9}{25p}$, so that Fourier sampling produces a value k, with $k-1$ being the closest integer to an integer multiple of $\frac{M}{p}$, with probability $\Omega(1)$. One of the convergents of the continued fraction expansion of $\frac{\lfloor \frac{jM}{p} \rceil}{M}$ is $\frac{j}{p}$, because $p^2 < M$. One computes the continued fraction expansion until one obtains the closest convergent to $\frac{\lfloor \frac{jM}{p} \rceil}{M}$, whose denominator is smaller than N; this denominator must be equal to p (see for example [17]). Since all these calculations can be done in polynomial time in the security parameter λ, one finds p in (quantum) polynomial time. □

Corollary 8. *Given a semigroup G, then $e(g)$ can be computed in polynomial time for any $g \in G$.*

To find $e(g)$, we need to compute g^{kp}, for any k satisfying $kp \geq i$. This can be done in polynomial time for $k = \lceil \frac{N}{p} \rceil$.

6 Decrypting in Ring Encryption Schemes

Our strategy for the computation of the decryption map of a ring homomorphic encryption scheme $(R, \mathbb{F}_2, \mathrm{Enc}, \mathrm{Dec})$ is based on the following commutative diagram:

$$\begin{array}{ccccc} R & \xrightarrow{e_R} & E(R) & \longrightarrow & \hat{E}(R) \\ & \searrow^{\mathrm{Dec}} & \downarrow \mathrm{D} & \swarrow_{\hat{\mathrm{D}}} & \\ & & \mathbb{F}_2 & & \end{array}$$

where D and $\hat{\mathrm{D}}$ are the restrictions of Dec to $E(R)$ and $\hat{E}(R)$, respectively, and e_R is the idempotent map. Indeed, since $\mathrm{Dec}(x^n) = \mathrm{Dec}(x)^n = \mathrm{Dec}(x)$, for any $x \in R$ and any positive integer n, we get that $\mathrm{Dec} = \mathrm{D} \circ e_R$. The commutativity of the other part of the diagram is equivalent to $\mathrm{Dec}(\hat{e}) = 1$. To prove it we show first that $\hat{E}(R)$ is nonempty. Notice that the morphism of rings $\mathrm{Dec} : \mathrm{R} \to \mathbb{F}_2$ factors over the morphism $\phi : R \to \prod_{i=1}^n \bar{R}_i/\mathfrak{m}_i$, so that the resulted morphism $\prod_{i=1}^n \bar{R}_i/\mathfrak{m}_i \to \mathbb{F}_2$, gives rise, for each i, to a morphism of fields $\bar{R}_i/\mathfrak{m}_i \to \mathbb{F}_2$, which is nontrivial only if $\bar{R}_i/\mathfrak{m}_i$ is isomorphic to $\mathbb{F}_2$, consequently $\hat{E}(R)$ is

nonempty, and Dec : R $\to \mathbb{F}_2$ factors over the morphism $\phi : R \to \prod_{j\in J} \bar{R}_j/\mathfrak{m}_j$. Since $\psi \circ \iota(\hat{e})$ is the unit of $\prod_{j\in J} \bar{R}_j/\mathfrak{m}_j$, we get that $\mathrm{Dec}(\hat{e}) = 1$.

By Proposition 4, D is a projection so that we need to find the coordinate $\mathbf{s} \in J$ that defines it. Unfortunately, even though $E(R)$ has a simple structure determined by its primitive idempotents, it is difficult, if not impossible, to compute them in polynomial time. So, rather than finding all primitive idempotents, we will concentrate on finding the primitive idempotent $e_{\mathbf{s}}$. For that, we compute first $\bar{e}$ and then $\hat{e}$.

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 $e \vee e'$. To find $\bar{e}$ we choose k random elements $x_1, ..., x_k \in R$, and we compute $e_R(x_1) \vee ... \vee e_R(x_k)$. It is easy to see that, for any $x \in R$, the primitive idempotent e_i occurs in the sum decomposition of $e_R(x)$ if and only if $x \notin \ker \phi_i$. Since ϕ_i is a ring homomorphism, this happens with probability $\geq \frac{1}{2}$. Consequently, the probability that e_i occurs in the sum decomposition of $e_R(x_1) \vee ... \vee e_R(x_k)$ is at least $1 - \frac{1}{2^k}$, and then

$$\Pr\left(e_R(x_1) \vee ... \vee e_R(x_k) = \bar{e}\right) \geq \prod_{i=1}^{n}(1 - \frac{1}{2^k}) > 1 - \frac{n}{2^k}.$$

So, if we choose $k > n + \lambda$ then the probability is at least $1 - \frac{1}{2^\lambda}$ (since we don't know n we can choose $k > \log_2 |R| + \lambda$), hence with overwhelming probability we have computed $\bar{e}$.

To find $\hat{e}$ we choose k random elements $x_1, ..., x_k \in R$ and we compute $e_R(x_1 - x_1^2) \vee ... \vee e_R(x_k - x_k^2)$. The primitive idempotent e_i occurs in the sum decomposition of $e_R(x - x^2)$ if and only if $\phi_i(x - x^2) \neq 0 \Leftrightarrow \phi_i(x) \notin \{0, 1\}$, hence this happens with probability $\geq \frac{1}{3}$ if $i \notin J$ (notice that $\phi_i(x - x^2) = 0$ for all $i \in J$). As above we have:

$$\Pr\left(e_R(x_1) \vee ... \vee e_R(x_k) = \sum_{i\notin J} e_i\right) \geq \prod_{i\notin J}\left(1 - \left(\frac{2}{3}\right)^k\right) > 1 - \frac{n - |J|}{1.5^k} > 1 - \frac{n}{1.5^k}.$$

This time, if we choose $k > \frac{\log_2 |R| + \lambda}{\log_2 3 - 1}$, we obtain $\sum_{i\notin J} e_i$ with overwhelming probability. Finally, we compute $\hat{e} = \bar{e} - \sum_{i\notin J} e_i$.

Proposition 6. *If $(R, \mathbb{F}_2, \mathrm{Enc}, \mathrm{Dec})$ is a commutative ring homomorphic encryption scheme with $\hat{E}(R) \simeq \mathbb{F}_2$, then the scheme is not resistant to quantum computing based attacks.*

Proof. If $\hat{E}(R) \simeq \mathbb{F}_2$ then $\hat{e}$ is a primitive idempotent and $e_{\mathbf{s}} = \hat{e}$, hence $\bar{R}_{\mathbf{s}} \simeq \bar{R}\hat{e}$ is a local Artin ring. Since Dec : $R \to \mathbb{F}_2$ factors over the homomorphism $f_{\mathbf{s}} : R \to \bar{R} \to \bar{R}\hat{e} \simeq \bar{R}_{\mathbf{s}}, x \mapsto x\hat{e}$, there exist a homomorphism $\mathrm{D}_{\mathbf{s}} : \bar{R}_{\mathbf{s}} \to \mathbb{F}_2$ such that $\mathrm{Dec}(x) = \mathrm{D}_{\mathbf{s}}(x\hat{e})$, $\forall x \in R$. Notice that $\mathrm{D}_{\mathbf{s}}(y) = 0$ if and only if $y \in \mathfrak{m}_s$, for all $y \in \bar{R}_{\mathbf{s}}$. Since $\mathfrak{m}_s$ is a nilpotent ideal, let k be the smallest positive integer such that $\mathfrak{m}_s^k = (0)$. Then, $\mathrm{Dec}(x) = 0$ iff $(x\hat{e})^m = 0$, for some $m \geq k$. If $\mathfrak{m}_s^i = \mathfrak{m}_s^{i+1}$ for some $0 \leq i \leq k - 1$, then by Nakayama's lemma ([2]), $\mathfrak{m}_s^i = (0)$, which is false. Hence, $|\mathfrak{m}_s^i/\mathfrak{m}_s^{i+1}| \geq 2$ for all $0 \leq i \leq k - 1$ so that $|\mathfrak{m}_s^{i+1}| \leq \frac{|\mathfrak{m}_s^i|}{2}$, therefore $|\mathfrak{m}_s^i| \leq \frac{|\bar{R}_{\mathbf{s}}|}{2^i} \leq \frac{|R|}{2^i}$. We obtain that $k \leq \lceil \log_2 |R| \rceil$, so that to decrypt $x \in R$ one computes $(x\hat{e})^m$ with $m = \lceil \log_2 |R| \rceil$. □

In general we have the following result:

Theorem 9. *Any commutative ring homomorphic encryption scheme is not quantum IND-CCA secure.*

Proof. In a sequence of randomly distributed elements of R about half of them are encryptions of 0, and with the help of the decryption oracle one finds which are those. In other words, we can produce a sufficiently large, uniformly distributed in R, set of encryptions of 0. As above, if the elements of this set are $x_1, ..., x_k$, then, with overwhelming probability, $\hat{e}(e_R(x_1) \vee ... \vee e_R(x_k))$ contains e_j with $j \in J \setminus \{s\}$ in its sum decomposition. In other words, with overwhelming probability, we have $\hat{e} - \hat{e}(e_R(x_1) \vee ... \vee e_R(x_k)) = e_{\mathbf{s}}$. Now, as above, to decrypt $x \in R$ one computes $(xe_s)^k$ with $k = \lceil \log_2 |R| \rceil$. If $(xe_s)^k = 0$ then $\mathrm{Dec}(x) = 0$, otherwise $\mathrm{Dec}(x) = 1$. □

Remark 10. *Since the encryption algorithm is public, one can use it to produce a sufficiently large set of encryptions of* 0 *as above. Unfortunately, one has no control on the frequency of apparition of such a ciphertext c, whose associated idempotent contains e_i, with $i \in I \setminus \{\mathbf{s}\}$, in its sum decomposition, equivalently $e_R(c) \cdot e_i = e_i$. Suppose that $f_{\mathbf{s}} = \hat{e} - \hat{e}(e_R(x_1) \vee ... \vee e_R(x_k))$, where $\{x_1, ..., x_k\}$ is a sufficiently large set of encryptions of* 0*. It is easy to see that if $c \in R$ is any ciphertext such that $e_R(c)(\bar{e} - f_{\mathbf{s}}) = e_R(c)$, then* $\mathrm{Dec(c)} = 0$*. On the other hand, if $e_R(c)(\bar{e} - f_{\mathbf{s}}) = e_R(c) - f_{\mathbf{s}}$, then* $\mathrm{Dec(c)} = 1$*. Unfortunately, if $f_{\mathbf{s}} \neq e_{\mathbf{s}}$, there are ciphertexts that do not satisfy neither the first nor the second equality. In this case, one can try to produce a new $f_{\mathbf{s}}$ by adding new encryptions of* 0 *to the set above. It is not clear how big the set of encryptions of zero has to be in order to get $f_{\mathbf{s}} = e_{\mathbf{s}}$ with overwhelming probability.*

7 Examples: Semigroup/Monoid Algebras

One of the natural constructions of rings with interesting idempotent structure is using semigroup/monoid algebras. In this section we shall study the properties of such rings from the cryptographic point of view.
For a semigroup G, we denoted by $G^0 := \coprod_{f \in E(G)} B_f^0$, which is a subsemigroup of G (see Proposition 3).

Definition 11. Let G be a semigroup. A subset $I \subseteq M$ is called 2-*invariant* if the map $x \mapsto x^2$ from I to I is a bijection.

In other words, the above map is a permutation of a 2-invariant set. In view of this definition we have:

Lemma 12. *Let G be a semigroup.*
i) If I is a 2-invariant subset of G, then $I \subseteq G^0$.
ii) $E(\mathbb{F}_2[G]) = \{\sum_{x \in I}[x] \mid I$ is 2-invariant$\}$.

Proof. The first claim is easy since for any element $x \in I$, there exist $k \geq 1$ such that $x^{2^k} = x$, therefore $x \in G^0$. The second claim follows easily from the definitions. Let us notice here that an $x \in G^0$ admits a $k \geq 1$ such that $x^{2^k} = x$, if and only if $p(x)$ is odd. □

An important application of the previous lemma is the following:

Proposition 7. *If G is a semigroup, then:*

$$E(\mathbb{F}_2[G^0]) = E(\mathbb{F}_2[G]) \text{ and } \hat{E}(\mathbb{F}_2[G^0]) = \hat{E}(\mathbb{F}_2[G]).$$

Here we identify $\mathbb{F}_2[G^0]$ with its image through the inclusion in $\mathbb{F}_2[G]$.

Proof. Only the second equality requires an argument. Due to the first equality we can identify the primitive idempotents of $\mathbb{F}_2[G]$ and $\mathbb{F}_2[G^0]$, let's say that these are $e_i, i \in I$. Then the local Artin factors that appear in the product decompositions of these two $\mathbb{F}_2$-algebras ar in fact the ideals generated by e_i, for each $i \in I$. For each $i \in I$, the inclusion $\mathbb{F}_2[G^0]e_i \to \mathbb{F}_2[G]e_i$ induces a homomorphism of their residue fields, which is injective. We claim that this homomorphism is also surjective. Indeed, notice that any element of G has a 2^k-power, for a sufficiently large k, that belongs to G^0, therefore the same is true for any element x of $\mathbb{F}_2[G]$, i.e. there exists some positive integer k such that $x^{2^k} \in \mathbb{F}_2[G^0]$. Then, we also have that $(xe)^{2^k} = (x)^{2^k}e \in \mathbb{F}_2[G^0]e$, in other words any element in the residue field of $\mathbb{F}_2[G]e$ has a 2^k-power that belongs to the residue field of $\mathbb{F}_2[G^0]e$. Since the residue field of $\mathbb{F}_2[G^0]e$ is a finite extension of $\mathbb{F}_2$, and the Frobenius morphism is surjective on any finite field, we get the claim. Since the inclusion map $\mathbb{F}_2[G^0] \to \mathbb{F}_2[G]$ induces isomorphisms for the residue fields of the corresponding local Artin factors, we get the second equality. □

The following proposition is an immediate consequence of Proposition 3 and Proposition 7:

Proposition 8. *If G is a semigroup, then we have an isomorphism of $\mathbb{F}_2$-vector spaces:*

$$E(\mathbb{F}_2[G]) \simeq \bigoplus_{f \in E(M)} E(\mathbb{F}_2[B_f^0]).$$

Notice that the above isomorphism is not an isomorphism of rings. What we can say about the image of the multiplication on the left hand side via the above isomorphism is that it preserves the structure given by the multiplication on $E(G)$, i.e. if $x \in E(\mathbb{F}_2[B_e^0])$ and $y \in E(\mathbb{F}_2[B_f^0])$ then $xy \in E(\mathbb{F}_2[B_{ef}^0])$. In view of the above facts, it is important we study the extremal cases, namely the case when $|E(G)| = 1$ and the case when $B_f^0 = \{f\}$ for all $f \in E(G)$, equivalently $G^0 = E(G)$. The general case deserves a separate analysis that we would carry on in a different paper. However, the two extremal cases are the building blocks for the general case.

7.1 One idempotent monoid algebra

Let M be a commutative semigroup consisting of only one block, that is $M = B_f$; equivalently $|E(M)| = 1$. In this case $M^0 := B_f^0$, which is a group. Using the decomposition theorem for abelian groups, there exist $C_1, ..., C_k$ cyclic groups such that $M^0 \simeq C_1 \times ... \times C_k$. Then we have an isomorphism of $\mathbb{F}_2$-algebras $\mathbb{F}_2[M^0] \simeq \mathbb{F}_2[C_1] \otimes_{\mathbb{F}_2} ... \otimes_{\mathbb{F}_2} \mathbb{F}_2[C_1]$. Suppose now that C is a cyclic group of order $N = 2^m \cdot N'$, where N' is odd and m is a non-negative integer. Then, we have the isomorphisms $\mathbb{F}_2[C] \simeq \mathbb{F}_2[X]/(X^N - 1) \simeq \mathbb{F}_2[X]/(X^{N'} - 1)^{2^m}$.

Next, we use the decomposition $X^{N'}-1=\prod_{d|N'}\Phi_d(X)$, where $\Phi_d(X)$ are the cyclotomic polynomials, to get an isomorphism:

$$\mathbb{F}_2[C]\simeq\prod_{d|N'}\mathbb{F}_2[X]/(\Phi_d(X))^{2^m}.$$

Next, let $\nu_2(d)$ be the order of 2 in the group $(\mathbb{Z}/d\,\mathbb{Z})^\times$. Then $\Phi_d(X)$ decomposes in $\mathbb{F}_2[x]$ into

$$\Phi_d(X)=\prod_{i=1}^{\phi(d)/\nu_2(d)}P_{i,d}(x),$$

where $P_{i,d}$ are irreducible distinct polynomials, all of degree $\nu_2(d)$. Using Chinese Remainder Theorem (in $\mathbb{F}_2[X]$), we get the following isomorphisms of $\mathbb{F}_2$-algebras:

$$\mathbb{F}_2[C]\simeq\prod_{d|N'}\prod_{i=1}^{\phi(d)/\nu_2(d)}\mathbb{F}_2[X]/(P_{i,d}(X))^{2^m}.$$

We have the following:

Lemma 13. *Let $Q_1(X),...,Q_k(X)\in\mathbb{F}_2[X]$ be irreducible polynomials, and $m_1,...,m_k$ non-negative integers. Then, there is a one-to-one correspondence between the local Artin factors of*

$$S(Q_1,...,Q_k;m_1,...,m_k):=\mathbb{F}_2[X]/(Q_1(X))^{2^{m_1}}\otimes_{\mathbb{F}_2}...\otimes_{\mathbb{F}_2}\mathbb{F}_2[X]/(Q_k(X))^{2^{m_k}},$$

and the local Artin factors of $S(Q_1,...,Q_k;0,...,0)$. In addition, corresponding factors have isomorphic residue fields.

Proof. Any maximal ideal of $S(Q_1,...,Q_k;m_1,...,m_k)$ contains the elements $1\otimes...\otimes P_i(X)\otimes...\otimes1$, for all $i\in\overline{1,k}$; let $\mathfrak{m}$ be the ideal generated by them. Since $S(Q_1,...,Q_k;m_1,...,m_k)/\mathfrak{m}\simeq S(Q_1,...,Q_k;0,...,0)$, the conclusion follows. □

Since tensor products commute with direct products, one is let to the following structure of group algebras:

Proposition 9. *Assume that the abelian group $M^0\simeq\prod_{j=1}^k\mathbb{Z}/N_j\,\mathbb{Z}$ with $N_j=2^{m_j}N'_j$, N'_j odd numbers and m_j non-negative integers for all j, then*

$$\mathbb{F}_2[M^0]\simeq\prod_{d_j|N'_j,\forall j}\prod_{i_j=1,\forall j}^{\phi(d_j)/\nu_2(d_j)}S(P_{i_1,d_1},...,P_{i_k,d_k};m_1,...,m_k).$$

We have the following consequence:

Corollary 14. *With the above notations, we have:*

$$\dim_{\mathbb{F}_2}(E(\mathbb{F}_2[M]))=\sum_{d_j|N'_j,\forall j}\frac{\prod_j\phi(d_j)}{\mathrm{lcm}_j(\nu_2(d_j))}.$$

Proof. Lemma 13 gives $E(S(P_{i_1,d_1},...,P_{i_k,d_k};m_1,...,m_k)) \simeq E(S(P_{i_1,d_1},...,P_{i_k,d_k};0,...,0))$. On the other hand, we have the isomorphisms:

$$S(P_{i_1,d_1},...,P_{i_k,d_k};1,...,1) \simeq \mathbb{F}_{2^{\nu_2(d_1)}} \otimes_{\mathbb{F}_2} ... \otimes_{\mathbb{F}_2} \mathbb{F}_{2^{\nu_2(d_k)}} \simeq \left(\mathbb{F}_{2^{\mathrm{lcm}_j(\nu_2(d_j))}}\right)^{\frac{\prod_j \nu_2(d_j)}{\mathrm{lcm}_j(\nu_2(d_j))}},$$

where the last isomorphism follows from Theorem 16.8 in [18]. Now, use Proposition 7 and Proposition 9 to get the result. □

We end this section with the following important result:

Theorem 15. *Let M be a commutative semigroup with only one block (e.g. abelian group), then*

$$\hat{E}(\mathbb{F}_2[M])) \simeq \mathbb{F}_2.$$

Consequently, any ring homomorphic encryption scheme over $\mathbb{F}_2$ with ciphertext space $\mathbb{F}_2[M]$ is not secure under quantum attacks.

Proof. One can see that the only factor of $S(P_{i_1,d_1},...,P_{i_k,d_k};0,...,0)$ isomorphic to $\mathbb{F}_2$ corresponds to $d_i = 1$ for all i, therefore occurs only once. Now, the conclusion follows from Proposition 7 and Proposition 9. □

7.2 Full idempotent monoid algebra

In this case, M is a commutative semigroup such that $M = E(M)$. We may suppose that M is a monoid because we may always add a neutral element. Since any element of $\mathbb{F}_2[M]$ is idempotent, we have that $E(\mathbb{F}_2[M]) = \mathbb{F}_2[M]$. On the other hand, we know from Proposition 4 that there exists an isomorphism $E(\mathbb{F}_2[M]) \simeq \mathbb{F}_2^n$ for some n. Counting the dimensions, we get that $n = |M|$. In addition, we obtain $\hat{E}(\mathbb{F}_2[M]) = E(\mathbb{F}_2[M]) = \mathbb{F}_2[M]$. To explicitly provide the isomorphism mentioned above, we need to seek primitive elements in $\mathbb{F}_2[M]$, as in the proof of Proposition 4. It is not quite easy to do this step and we shall provide next the answer for the case where M is a free idempotent monoid.

We identify M with the free monoid $(\mathbb{F}_2^k, \cdot)$, so that let $e_i = (0,\ldots,1,\ldots 0)$, where 1 is in the i^{th} position. For any subset $A \subseteq \{1,\ldots,k\}$, let $e_A := \sum_{i\in A} e_i$ (here the sum is considered in the $\mathbb{F}_2$-algebra $\mathbb{F}_2^k$). Also, for any subset $S \subseteq \{1,\ldots,k\}$, we define $E_S := \sum_{A\subseteq S}[e_A] \in \mathbb{F}_2[M]$. By convention, $E_\emptyset := [\mathbf{0}]$.

Proposition 10. *We have an isomorphism of $\mathbb{F}_2$-algebras:*

$$\mathbb{F}_2[M] \simeq \bigoplus_{S\subseteq\{1,...,k\}} \mathbb{F}_2 \cdot E_S.$$

Proof. The only thing we need to check is that the idempotents E_S form an orthogonal basis. The number of these elements coincide with the dimension $\dim_{\mathbb{F}_2} \mathbb{F}_2[M] = 2^k$. Thus we need only to check the orthogonality relations. So let's consider S and T two different subsets of $\{1,\ldots,k\}$. Then:

$$E_S \cdot E_T = \sum_{A\subseteq S,\ B\subseteq T} [e_A][e_B] = \sum_{A\subseteq S,\ B\subseteq T} [e_{A\cap B}] = \sum_{C\subseteq S\cap T} [e_C] \sum_{A\subseteq S,\ B\subseteq T,\ A\cap B=C} 1.$$

We claim that the last sum is always even (i.e. 0 in $\mathbb{F}_2$). Since the relation is symmetric in S and T, we may assume that there exists $x \in S \setminus T$. In particular, $x \notin C$. Then, in the last sum, the subsets A that do not contain x and $A \cup \{x\}$ both are counted for any fixed subset B. The claim is now obvious. □

8 Conclusions

• In the present work we are only interested in ring homomorphic schemes over $\mathbb{F}_2$ since those are exactly the schemes that produce FHE schemes. If one is interested in general ring encryption schemes, then one has to consider the case in which the plaintext space is an arbitrary ring.
• Our analysis is restricted to the commutative case. Some of the results may extend to the noncommutative case, but it is beyond the scope of this article. The reader might have observed already that in fact the structure of ring homomorphic encryption schemes is actually governed solely by the *existence* of the decryption algorithm. However in *constructing* ring homomorphic encryption schemes, one needs an efficient encryption algorithm and this is usually the innovative part in such constructions. Thus, this article can be viewed as a negative result in the sense it shows how *not* to construct a ring homomorphic encryption scheme. Moreover, if one wants to construct such a scheme in the post-quantum era, then such thing is virtually impossible in the commutative case.
• Although we prove that under mild hypothesis ring homomorphic encryptions are not quantum secure, there is no example of ring homomorphic encryption scheme (enjoying all the good features) that enjoys classical security. If one relax some of the conditions imposed for ring homomorphic encryption schemes, then one can find such examples. In [4] there are two examples based on monoid algebras where there is only one relaxation in the initial conditions: "compact" is replaced by "bounded".
• The main novelty of this article (compared with other quantum attacks such as in [1]) is that we use quantum computation to find a (pseudo)-secret key which is used afterwards classically for decryption.
• As we mentioned in the Introduction, the IND-CCA security can be replaced by IND-CPA security using the δ-covering subgroups. The probability of the pseudo secret key to be the real secret key(i.e. of decrypting correctly any cyphertext) depends on the chosen δ.

References

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

[2] Atiyah, M. F.; Macdonald, I. G.: *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[3] Armknecht, F.; Katzenbeisser, S.; Peter, A.: *Group Homomorphic Encryption: Characterizations, Impossibility Results, and Applications* in Designs, Codes and Cryptography, Volume 67, Number 2, 2013, pp. 209–232.

[4] Barcau, M.; Paşol, V.: *Fully Homomorphic Encryption from Monoid Algebras*, preprint.

[5] Brakerski, Z.; Vaikuntanathan, V.: *Efficient fully homomorphic encryption from (standard) LWE*, In IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, Rafail Ostrovsky editor, pp. 97 - 106.

[6] Brakerski, Z.: *Fully homomorphic encryption without modulus switching from classical GapSVP*, In CRYPTO 2012, pp. 868 - 886.

[7] 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.

[8] Childs, A.M.; Ivanyos, G.: *Quantum computation of discrete logarithms in semigroups*, Journal of Mathematical Cryptology, Volume 8, Number 4, 2014, pp. 405-416.

[9] Childs, A.M.; van Dam, W.: *Quantum algorithms for algebraic problems*, Reviews of Modern Physics 82, 2010, pp. 1 - 52.

[10] Coron, J-S., Mandal, A., Naccache, D., Tibouchi, M.: *Fully homomorphic encryption over the integers with shorter public keys*, P. Rogaway editor, Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara 2011, Lecture Notes in Computer Science, vol. 6841, Springer, 2011, pp. 487 - 504.

[11] van Dijk, M.; Gentry, C.; Halevi, S.; Vaikuntanathan, V.: *Fully homomorphic encryption over the integers*, In EUROCRYPT, 2010, pp. 24 - 43. Full Version in http://eprint.iacr.org/2009/616.pdf.

[12] Gentry, C.: *A fully homomorphic encryption scheme*, PhD thesis, Stanford University, 2009.

[13] 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.

[14] Gentry, C.: *Computing arbitrary functions of encrypted data*, Communications of the ACM, Vol. 53, Issue 3, March 2010, pp. 97 - 105.

[15] Gentry, C., Halevi, S.: *Fully homomorphic encryption without squashing using depth-3 arithmetic circuits*, In IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, Rafail Ostrovsky editor, pp. 107 - 109.

[16] Gentry, C., Sahai, A., Waters, B.: *Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based*, Advances in Cryptology - CRYPTO 2013, Lecture Notes in Computer Science, Vol. 8042, 2013, pp. 75 - 92.

[17] Hardy, G.H.; Wright, E.M.: *An Introduction to the Theory of Numbers*, Oxford University Press, 5th edition.

[18] McDonald, B.R.: *Finite Rings with Identity*, Pure and Applied Mathematics 28, Marcel Dekker Inc., New York, 1974.

[19] Ostrovsky, R.; Skeith III, W.E.: *Communication Complexity in Algebraic Two-Party Protocols*, In Proceedings of CRYPTO 2008, LNCS 5157, 2008, pp.379 - 396.

[20] 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.

[21] Regev, O.: *Lattice-based cryptography*, In Advances in Cryptology-CRYPTO, Springer, 2006, pp. 131-141.

[22] Sen, J.: *Homomorphic Encryption: Theory & Application.*

[23] 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.

[24] Smart, N., Vercauteren, F. *Fully homomorphic encryption with relatively small key and ciphertext sizes*, In P. Nguyen and D. Pointcheval, editors, Public Key Cryptography, vol. 6056 of Lecture Notes in Computer Science, Springer, 2010, pp. 420 - 443.

Mugurel Barcau, Researcher, CertSign S.A., Bucharest, Romania
and
Institute of Mathematics of the Romanian Academy "Simion Stoilow", Str. Grivitei 21, Bucharest, Romania
E-mail address: barcau@yahoo.com

Vicenţiu Paşol, Researcher, CertSign S.A., Bucharest, Romania
and
Institute of Mathematics of the Romanian Academy "Simion Stoilow", Str. Grivitei 21, Bucharest, Romania *E-mail address*: vpasol@yahoo.com