THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 21, Number 1/2020, pp. 3–10

ON THE IND-CPA SECURITY OF RING HOMOMORPHIC ENCRYPTION SCHEMES OVER $\mathbf{F}_2$

Mugurel BARCAU[1,2], Vicențiu PAȘOL[1,2]

[1] certSIGN – Research and Development, Bucharest, Romania
2 Institute of Mathematics "Simion Stoilow" of the Romanian Academy
Corresponding author: Mugurel BARCAU, E-mail: mugurel.barcau@imar.ro

Abstract. In this paper we shall construct an attack that breaks the IND-CPA security of any ring homomorphic encryption scheme over $\mathbf{F}_2$. We generate a subring of 2-power characteristic in the ciphertext space using any encryption of 1. In the idempotent decomposition of this subring constructed by the authors in a previous work [4], there exist a (unique) primitive idempotent that can be used as a secret key to compute the decryption of any ciphertext. We compute with high probability a good approximation of this secret key using the ideas proposed in [1]. Quantum computations are solely used in the first part of the algorithm that computes the subring of 2-power characteristic. All the other algorithms are classical. The approximation of the "secret key" is used to find the projection of any ciphertext which, with high probability, reveals the plaintext. In particular, there exist a classical PPT algorithm that breaks the IND-CPA security of any ring homomorphic encryption scheme over $\mathbf{F}_2$ with ciphertext space a unital ring of 2-power characteristic.

Key words*:* public key encryption, homomorphic encryption schemes, quantum algorithms.

1. INTRODUCTION

Many sensitive data need to be protected and analyzed without leaking any information to the potentially evil parties. For this reason, working with encrypted data is necessary for a lot of practical applications. Without any doubt, one of the most useful tools for creating solutions in this sense is the Fully Homomorphic Encryption (FHE). Basically, it provides a way of encrypting data and performing any computation on encrypted data, without revealing at any point the data in clear. The work in this area exploded after the pioneering Ph.D. thesis of C. Gentry who was the first to introduce a procedure for creating FHE schemes (see [7,8]). However, all of the existing schemes are error-based encryption schemes, i.e. some noise (error) is added to fresh encryptions in order to insure privacy. The downside is that the error accumulates, and at some point will make the encrypted data unreadable (the decryption algorithm will not perform correctly). This is why, an additional algorithm, called bootstrapping, is necessary in order to reduce the accumulated noise. Usually this algorithm is costly and it makes the scheme less efficient. In the view of the great progress in the technology of quantum computers, one has to analyze the security of such schemes under a potential attacker that has at his disposal such technologies. Nowadays, it is believed that some of these schemes are quantum resistant, even though much work has been put forward for denying this statement.

On the other hand, some natural questions arise: is there a noise-free FHE and if so, how efficient and secure can it be? What if the attacker has only limited access to quantum computations, is such a scheme still secure? A partial answer to the first question was provided in [5], where such schemes were constructed, but the compactness condition was replaced by a weaker boundedness condition. In this paper, we provide a negative answer to the second question for a large class of such schemes. Ring homomorphic encryption schemes over $\mathbf{F}_2$ are not IND-CPA secure against an attacker that has access to only few quantum computations (to be more precise, two quantum experiments are necessary to be performed in the first phase of the IND-CPA experiment). Even though our set-up is restricted to the boolean plaintext, the results can be generalized with no other new ideas needed.

1.1. Related work

The security of the known error-based FHE schemes, was considered in many papers, among which we mention [6] and [9]. It has been shown that these schemes are not IND-CCA^1 secure. On the other hand, the security of ring homomorphic encryption schemes was considered in [3,4], where it has been shown that these schemes are not IND-CCA^1 secure and in certain cases key-recovery attacks were presented. In [1] an IND-CPA attack is presented on group homomorphic encryption schemes. Since any ring homomorphic encryption scheme gives rise to a group homomorphic encryption scheme by forgetting the multiplicative structure on both the ciphertext and plaintext spaces, this IND-CPA attack may be used in the case of a ring homomorphic encryption scheme, but is much less efficient than our attack on one hand, and on the other hand is based on the existence of a set of generators of the ciphertext space (viewed as an abelian group). Our attack does not assume anything about the ciphertext space. Moreover, we use quantum computations only in the first phase of the IND-CPA experiment, when we compute a certain idempotent. Then, using similar ideas as in [1], we compute a "secret key" which is used to decrypt ciphertexts using classical algorithms. In contrast, the attack in [1] uses quantum computations in both phases of the IND-CPA experiment, in other words uses quantum computations to decrypt each ciphertext that encodes each bit of information, and for this reason their attack is almost impractical, at least in the near future.

1.2. Our contribution

As it is recalled in Section 3, any ring homomorphic encryption scheme over $\mathbf{F}_2$ possesses a theoretical decryption key, no matter how the decryption algorithm works. In the absence of the decryption oracle, there is no way of finding this key without any additional information about the decryption algorithm. Our strategy is to find a pseudo-key that approximates the theoretical decryption key and then show that this pseudo key can be used to break the IND-CPA security of the scheme. In fact, one is able to choose how good the approximation can be, which, in a limiting process, is equivalent to a key-recovery attack.

1.3. Plan of the paper

In Section 2 we recall the definitions and notations used for the rest of the paper. Section 3 is dedicated to the presentation of some useful facts about the structure of finite commutative rings and their applications to ring homomorphic encryption schemes. Finally, in Section 4 we present the cryptanalysis of ring homomorphic encryption schemes over $\mathbf{F}_2$, mentioning every time which computations/algorithms are needed, if they are quantum or classical.

2. DEFINITIONS AND NOTATIONS

Let us define ring homomorphic encryption schemes, which is the main object of study in this work. Throughout this paper we use λ to indicate the security parameter. Since a ring homomorphic encryption scheme is a particular type of a homomorphic encryption scheme, we define first these schemes.

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

$$HE = \left(HE.KeyGen, HE.Enc, HE.Dec, HE.Eval\right)$$

is a quadruple of PPT algorithms as follows:

- **Key Generation.** The algorithm $(pk, evk, sk) \leftarrow HE.KeyGen(1^\lambda)$ 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* $c \leftarrow HE.Enc_{pk}(m)$ takes the public key pk and a single message m and outputs a ciphertext c.

- **Decryption.** The algorithm $m^\star \leftarrow HE.Dec_{sk}(c)$ takes the secret key sk and a ciphertext c and outputs a message $m^\star$.
- **Homomorphic Evaluation.** The algorithm $c_f \leftarrow HE.Eval_{evk}(f, c_1, ..., c_\ell)$ 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.

A HE scheme is $\mathcal{C}$-homomorphic for a class of circuits $\mathcal{C} = \{\mathcal{C}_\lambda\}_{\lambda \in \mathbf{N}}$, 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

$$Pr\left[HE.Dec_{sk}\left(HE.Eval_{evk}(f_\lambda, c_1, ..., c_\ell) \neq f_\lambda(\mu_1, ..., \mu_\ell)\right)\right] = negl(\lambda), \tag{1}$$

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

Moreover, 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 bit long, regardless of f or the number of inputs.

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

We introduce now ring homomorphic encryption schemes:

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

1. $Dec_\lambda(sk, c) = m$, for any $c \leftarrow Enc_\lambda(pk, m)$,

2. the scheme is compact as a homomorphic encryption scheme.

Notice that compactness condition is equivalent in this situation to the existence of two representations: $R_\lambda \xrightarrow{\iota_R} \{0,1\}^{n_R(\lambda)}$, $S_\lambda \xrightarrow{\iota_S} \{0,1\}^{n_S(\lambda)}$, such that:

1. Decryption $Dec_\lambda : \iota_R(R_\lambda) \to \iota_S(S_\lambda)$ is a deterministic polynomial time algorithm.

2. Encryption $Enc_\lambda : \iota_S(S_\lambda) \to \iota_R(R_\lambda)$ is a probabilistic polynomial time algorithm.

Throughout this paper, we will assume that the finite ring R_λ, i.e. the ciphertext space of a ring homomorphic encryption scheme is a commutative ring, and that the plaintext space S_λ is the field with two elements. To show that such a ring homomorphic encryption scheme is a fully homomorphic encryption scheme, one has to replace any gate of a boolean circuit with the corresponding ring operation and use the homomorphicity of the decryption map.

We briefly recall the only security notion that we need in this paper, that is indistinguishability under chosen-plaintext attack ($IND-CPA$) 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 $IND-CPA$:

– Phase One: Generate a pair of keys $(pk, sk) \leftarrow HE.KeyGen(1^\lambda)$. $\mathcal{A}$ starts its computation and proposes two messages m_0 and m_1.

– Phase Two: Choose at random a bit i, and compute $c \leftarrow HE.Enc_{pk}(m_i)$. Give c to $\mathcal{A}$, and let $\mathcal{A}$ continue its computation.

– Let m' be $\mathcal{A}$'s output. Output 1 if $m' = m_i$ and 0 otherwise.

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

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

We shall also say that a scheme is quantum-classical $IND-CPA$ 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 $IND-CPA$ security etc.

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

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

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

3. FINITE COMMUTATIVE RINGS

In this section we recall the results of [3,4] about the structure of finite commutative rings and applications of these results to ring homomorphic encryption schemes. For any ring R let $E(R)$ be the subset of R consisting of all idempotent elements. Notice that $E(R)$ is a subsemigroup of the multiplicative semigroup $(R,\cdot)$. Moreover, if one defines addition in $E(R)$ by: $e\oplus e'=e+e'-2ee'$, $\forall e,e'\in E(R)$, then $E(R)$ becomes a ring of characteristic 2. It is shown in [3], that if R is a finite commutative ring then there is a well defined map $e:R\to E(R)$, which is a homomorphism of multiplicative semigroups. Indeed, for any $x\in R$ the sequence $(x^n)_{n\geq 1}$ is preperiodic, so that if t is the length of the tail and p the period then $e(x)=x^{kp}$, where k is any positive integer such that $kp\geq t$. The following result is a consequence of Corollary 8 from [3] and Proposition 3 from [4]:

PROPOSITION 1. *For any finite commutative ring R there is an efficient polynomial time quantum algorithm that computes the map $e:R\to E(R)$. Moreover, when R is a ring of prime power characteristic the map e can be computed classically.*

If R is a finite commutative BBR defined by the generating set $G=\{g_1,...,g_d\}$, then we compute

$$\bar{e} := \overset{d}{\underset{j=1}{\vee}} e(g_j) \tag{3}$$

where the operation $e \vee e' := e \oplus e' \oplus ee'$ is commutative and associative. Then we have (Theorem 2 in [4]):

THEOREM 1. *Let R be a finite commutative ring and let $\bar{R} := R\bar{e}$, $N_R := \{x \in R \mid x \cdot \bar{e} = 0\}$. Then*
1. *$\bar{R}$ is a unital subring of R, and N_R is a nilpotent ideal, hence subring of R.*
2. *There is an isomorphism of rings $R \cong \bar{R} \times N_R$, $x \mapsto (x\bar{e}, x - x\bar{e})$.*
3. *Any morphism of rings $S \to R$ with S unital, factors as $S \to \bar{R} \subseteq R$.*

Since $\bar{R}$ is a finite commutative unital ring the structure theorem for Artin rings (Theorem 8.7 in [2]) asserts that $\bar{R}$ is isomorphic to a product of local Artin rings, so that we have:

$$R \cong R_1 \times ... \times R_n \times N_R \tag{4}$$

where R_i's are local rings. Notice that each local Artin component R_i is of the form Re_i, where e_i is a (primitive) idempotent, and $\bar{e} = e_1 + ... + e_n$. In particular, we obtain $E(R) \cong E(R_1) \times ... \times E(R_n) \cong \mathbf{F}_2^n$. It is shown in Theorem 3 [4] that any nontrivial ring homomorphism $\phi : E(R) \to \mathbf{F}_2$ is the projection on the i-th coordinate, for some $i \in \{1,...,n\}$. Moreover, any ring homomorphism $\phi : R \to \mathbf{F}_2$ factorizes as $R \to Re_s \to \mathbf{F}_2$, where Re_s is a local ring with residue field isomorphic to $\mathbf{F}_2$. Consequently, if $(R, \mathbf{F}_2, Dec, Enc)$ is a ring homomorphic encryption scheme to compute Dec it is enough to find e_s. Indeed, for any $x \in R$, $Dec(x) = 0$ if and only if $(xe_s)^m = 0$ for sufficiently large m (for more details see Section 4).

We recall the following result from [3]:

THEOREM 2. *Let $(R, \mathbf{F}_2, Dec, Enc)$ be a ring homomorphic encryption scheme such that R is a BBR isomorphic to a group algebra over $\mathbf{F}_2$, i.e. there exist an abelian group G such that $R \cong \mathbf{F}_2[G]$. Then the scheme is not IND-CPA secure.*

The *proof* is based on the fact that there exist a unique primitive idempotent e with residue field isomorphic to $\mathbf{F}_2$, so that it must be e_s. Since R is in this case a ring of characteristic 2 the computation of the map $e : R \to E(R)$ can be done classically, i.e. no quantum algorithm is needed (Proposition 1). One computes e_s and then uses it as above to decrypt correctly any ciphertext, which means that we have in fact a key-recovery attack for such schemes.

Remark. The main result of this paper extends the above result. We show that a ring homomorphic scheme is not *IND-CPA* secure if R is any finite commutative ring that is a ring oracle. In other words, we do not assume that a generating set for R is given.

4. IND-CPA ATTACK

Suppose that $(R, \mathbf{F}_2, Dec, Enc)$ is a ring homomorphic encryption scheme and $\mathcal{A}$ a polynomial time adversary. The strategy of $\mathcal{A}$ is as follows: it constructs first a subring R_2 of R and a map $\pi_2 : R \to R_2$ such that $Dec(x) = Dec(\pi_2(x))$. Moreover, the subring R_2 enjoys the additional property that is a unital ring of 2-power characteristic. As a consequence, the map $e : R_2 \to E(R_2)$ can be computed classically. Thus, once R_2 is constructed no more quantum algorithms are needed for the rest of the attack.

To achieve the above construction, the adversary $\mathcal{A}$ will do the following computations:

1. Let c be any encryption of 1.

2. Compute $e' := e(c)$. This is done using the quantum algorithm from Proposition 1.

3. Compute $p(e') := \min\{n \mid n \cdot e' = 0_R\}$. The adversary uses Shor's quantum algorithm (see [10]).

4. Compute $v_2\left(p(e')\right)$ and $n_1, n_2 \in \mathbf{Z}$ such that $2^{v_2(p(e'))} \cdot n_1 + \frac{p(e')}{2^{v_2(p(e'))}} \cdot n_2 = 1$.

   Set $e_2 := \frac{p(e')}{2^{v_2(p(e'))}} \cdot n_2 \cdot e'$. This is just an application of the Euclidean algorithm.

5. Set $R_2 := R \cdot e_2$.

Notice that the map π_2 is computed by $\pi_2(x) = x \cdot e_2$.

As explained in the previous section there exists a unique primitive idempotent $e_s \in R_2$ such that $Dec(e_s) = 1$. Consequently, $Dec(x) = 0$ if and only if $e(xe_s) = 0$. Indeed, $Dec(x) = Dec(xe_s) = Dec\left(e(xe_s)\right)$. Notice that $E(R_2 e_s) = \{0, e_s\}$ so that $Dec\left(e(xe_s)\right) = 0$ if and only if $e(xe_s) = 0$, equivalently $(xe_s)^m = 0$ for sufficiently large m. Unfortunately, with no additional information provided by a decryption oracle which is not accessible in the IND-CPA experiment, one is unable to find generically e_s. The strategy of $\mathcal{A}$ is to find a "good approximation" of e_s. This means to find and idempotent f_s such that, with overwhelming probability,

$$e\left(Enc(0) \cdot f_s\right) = 0.$$

This will be achieved by removing enough primitive idempotents that decrypt to 0 from the primitive idempotent decomposition of e_2.

The following classical algorithm computes an approximation of e_s:

ALGORITHM 1. Compute an approximation of e_s

```
$e_{1,0} := e_2$
    **for** $i = 1$ to $t$ **do**
        **for** $k = 1$ to $N$ **do**
            $e_{i,k} := e_{i,k-1} - e\left(Enc(0) \cdot e_{i,k-1}\right)$
        **end for**
        $e_{i+1,0} := e_{i,N}$
    **end for**
**return** $f_s := e_{t+1,0}$
```

The following result proves the correctness of the above algorithm, i.e. that it produces a "good approximation" of e_s.

THEOREM 3. *Let* $\left(R, \mathbf{F}_2, Dec, Enc\right)$ *be a ring homomorphic encryption scheme. Fix two values* $0 < \delta, \epsilon < 1$ *and set* $t := \left\lceil \log_2 |R| \right\rceil - 2$, $N := \left\lceil \frac{\log(1-\epsilon) - \log(t)}{\log(\delta)} \right\rceil$. *Then the above algorithm outputs with a probability greater than* ϵ *an idempotent* f_s *such that* $Pr\left[e\left(Enc(0) \cdot f_s\right) = 0\right] > \delta$.

Proof. Assume that $e_{i+1,0}=e_{i,0}$ for some $1\le i\le t$. This means that at step i, for all N encryptions of 0 one has $e\left(Enc(0)\cdot e_{i,0}\right)=0$. Assume that $Pr\left[e\left(Enc(0)\cdot e_{i,0}\right)=0\right]=\delta'\le\delta$, otherwise we are done. Then the probability that this happens at the i^{th} step equals $\delta'^{N}\le\delta^{N}$. Hence, the probability of this happening in all of the t steps is less than $t\cdot\delta^{N}\le 1-\epsilon$.

Notice that, if each of the steps produces a different $e_{i+1,0}$, then the number of primitive idempotents in the decomposition decreases with at least one at each step. But this means that $e_{t+1,0}=f_s=e_s$, in which case $Pr\left[e\left(Enc(0)\cdot f_s\right)=0\right]=1$.

Now we can state and prove the main result:

THEOREM 4. *Any ring homomorphic encryption scheme over* $\mathbf{F}_2$ *is not quantum-classical IND-CPA secure.*

Phase One: The adversary $\mathcal{A}$ computes R_2 as in the beginning of the section, and then $\mathcal{A}$ computes f_s as in Algorithm 1.

Phase Two: Let b be a random bit $b\in\{0,1\}$ and let $c_b\leftarrow Enc(b)$. The adversary $\mathcal{A}$ computes $e(c_b\cdot f_s)$, and outputs $b'=0$ if $e(c_b\cdot f_s)=0$, otherwise outputs $b'=1$.

With probability $(1+\epsilon\delta)/2$ the attacker wins the game. Indeed, the Algorithm 1 outputs a “good approximation” of e_s with probability ϵ. In this case, the probability $Pr\left[b'=b\right]\ge\frac{1}{2}\delta+\frac{1}{2}$. However, even in the case of "bad approximations" the probability of correct decryption is at least $\frac{1}{2}$. Thus, overall, the probability $Pr\left[b'=b\right]$ is at least $\epsilon\cdot\frac{\delta+1}{2}+(1-\epsilon)\frac{1}{2}=\frac{\epsilon\delta+1}{2}$.

We want to stress that the quantum computations were used solely to compute R_2, thus no quantum computations are needed during the second phase of the IND-CPA experiment.

Also, in practice, once the Algorithm 1 is performed, one can redefine the input e_2 for further applications of the same algorithm by $e_2 := f_s$. This means that we may start with an idempotent that has fewer primitive idempotents in its decomposition already. In other words, the attacker gets better and better with each use of Algorithm 1.

In particular, we have:

THEOREM 5. *Any ring homomorphic encryption scheme over* $\mathbf{F}_2$ *with ciphertext space a unital ring oracle of 2-power characteristic is not classical-classical IND-CPA secure.*

Indeed, one can take R_2 to be R.

ACKNOWLEDGEMENT

The second author was (partially) supported by a grant of Romanian Ministry of Research and Innovation, CNCS - UEFISCDI, project number PN-III-P4-ID-PCE-2016-0157, within PNCDI III.

REFERENCES

1. F. ARMKNECHT, T. GAGLIARDONI, S. KATZENBEISSER, A. PETER, *General impossibility of group homomorphic encryption in the quantum world,* International Workshop on Public Key Cryptography – PKC 2014, Lecture Notes in Computer Science, **8383**, pp. 556-573, 2014.

2. M.F. ATIYAH, I.G. MACDONALD, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, MA, 1969.
3. M. BARCAU, V. PASOL, *Ring homomorphic encryption scheme*s, available at https://eprint.iacr.org/2018/583.pdf, December 2019.
4. M. BARCAU, V. PASOL, *Cryptanalysis of ring homomorphic encryption schemes,* available at https://eprint.iacr.org/2019/594.pdf, December 2019.
5. M. BARCAU, V. PASOL, *Bounded fully homomorphic encryption from monoid algebras,* available December 2019 at https://eprint.iacr.org/2018/584.pdf.
6. M. CHENAL, Q. TANG, *On key recovery attacks against existing somewhat homomorphic encryption schemes,* International Conference on Cryptology and Information Security in Latin America – LATINCRYPT 2014, Lecture Notes in Computer Science, **8895**, pp. 239-258, 2014.
7. C. GENTRY, *A fully homomorphic encryption scheme,* PhD Thesis, Stanford University, 2009.
8. C. GENTRY, *Fully homomorphic encryption using ideal lattices*, Proceedings of the 41st annual ACM symposium on Theory of computing, pp. 169-178, 2009.
9. K. LOFTUS, A. MAY, N.P. SMART, F. VERCAUTEREN *On CCA-secure somewhat homomorphic encryption*, International Workshop on Selected Areas in Cryptography – SAC 2011, Lecture Notes in Computer Science, **7118**, pp. 55-72, 2011.
10. P.W. SHOR, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Journal on Computing, **26**, 5, pp. 1484-1509, 1997.

Received June 27, 2019