TWMS J. App. Eng. Math. V.9, N.1, Special Issue, 2019, pp. 151-158

# ON KEY EXCHANGE METHOD VIA TOPOLOGICAL CONCEPTS

K. POLAT[1], §

Abstract. Key exchange algorithms such as the Diffie-Hellman method are used to determine a common secret key which will be used in symmetric key algorithms in cryptography. In this paper, we give a key exchange algorithm which includes some steps of Diffie-Hellman method by using algorithms of the topological basic concepts such as subbase, base and topology.

Keywords: cryptography, Diffie-Hellman method, key exchange algorithms, topology.

AMS Subject Classification: 11T71, 54H99

## 1. INTRODUCTION

Cryptography which comes from the Greek words *kryptos* meaning secret and *graphikos* meaning to write is a study of methods for receiving and sending confidential messages that the intended recipient can decrypt and read [5].

The earliest documented encryption used so far was used by the Roman army during the Julian Caesar period in the 60s BC. This encryption is called *Ceaser Cipher* which is a special shift cipher in which a plain text is encrypted by shifting each character in this text by a key number.

Symmetric key algorithms are a set of cryptographic algorithms that perform both encryption and decryption by using the same or similar keys, that is keys that are the same or can be converted to each other by a simple method while asymmetric key algorithms is a set of cryptographic algorithms in which different keys are used for encryption and decryption operations [3].

Diffie-Hellman key exchange is a special method used to exchange cryptographic keys. This is one of the first practical key exchange examples applied in the field of cryptography. The Diffie-Hellman key exchange method allows two persons to obtain a common secret key over insecure media. This key can then be used to encrypt the communication from an unsecured channel using a symmetric key cipher [2].

In this paper, by using the algorithms of the basic concepts of topology such as subbase, base and topology, we have developed a key exchange method that includes some steps of the Diffie-Hellman key exchange method. Readers can refer to the references [1, 4] for detailed information on this topological concepts.

[1] Department of Mathematics, Faculty of Science and Letters, Agri Ibrahim Cecen University, 04100, Agri, Turkey.
e-mail: kadirhanpolat@agri.edu.tr; ORCID: https://orcid.org/0000-0002-3460-2021;

§ Selected papers of International Conference on Life and Engineering Sciences (ICOLES 2018), Kyrenia, Cyprus, 2-6 September, 2018.

## 2. SOME ALGORITHMS

### 2.1. Class Ordering Algorithm.

**Definition 2.1.** *Given an finite class $\mathcal{A}$ whose each element consists of natural numbers. A relation $\leq$ on $\mathcal{A}$ defined by, for every pair of sets $A \neq B \in \mathcal{A}$,*

$$A \leq B \Leftrightarrow |A| < |B| \vee (\min\{A \setminus B\} \leq \min\{B \setminus A\})$$

*is called* a class ordering. *The* class ordering number of a set $A$ in $\mathcal{A}$ *is the sequence number of $A$ between elements of $\mathcal{A}$ by the relation $\leq$. $A$ is to be said* the $n$-th element of $\mathcal{A}$ *if class ordering number of a set $A$ in $\mathcal{A}$ is $n$.*

**Example 2.1.** *Given a class*

$$\mathcal{A} = \{\{1,3,5,7\},\{1\},\{1,2,6\},\{1,3\},\{1,3,6\},\{1,4\},\{2\},\{1,2,5\}\}.$$

*Then, the class ordering on $\mathcal{A}$ is as follows:*

$$\{1\} \leq \{2\} \leq \{1,3\} \leq \{1,4\} \leq \{1,2,5\} \leq \{1,2,6\} \leq \{1,3,6\} \leq \{1,3,5,7\}.$$

*Therefore, The set $\{1\}$ is the first element of $\mathcal{A}$ while $\{1,3,5,7\}$ is the last element of $\mathcal{A}$. Also, The set $\{1,2,5\}$ is the fifth element of $\mathcal{A}$.*

The class ordering described above is given in Algorithm 1 by using Mathematica script language.

```
ClassOrdering[x_, y_] := Module[{result = False},
    If[Length[x] < Length[y]||
      (Length[x] == Length[y]∧
      Min[Complement[x, y]] < Min[Complement[y, x]]),
        result = True
    ];
    result
];
```

**Algorithm 1:** ClassOrdering Algorithm

The ClassOrdering function compares the sets x and y given as its inputs by class ordering defined above, and gives True if $x \leq y$, otherwise False as output.

**Example 2.2.** *In order to sort the class*

$$\mathcal{A} = \{\{1,2\},\{1,3\},\{2,3\},\{1,3,4\},\{1\},\{2\},\{3\}\}$$

*by class ordering we call the function $Sort[\mathcal{A}, ClassOrdering]$ in Mathematica and get the output*

$$\{\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,3,4\}\}.$$

2.2. **CardOrd Algorithm.** Given a set $A$ with the cardinal n. Let $K$ be the $k$-th subset of $A$ based on the class ordering according to the power set of $A$. When the algorithm, called CardOrd, given in Algorithm 2 by using the Mathematica script language gets the values $n$ and $k$, respectively, as inputs, it gives the pair $\{m, r\}$ as outputs where $m$ denotes $|K|$ and $r$ denotes the class ordering number of $K$ in the set of the subsets of $A$ with the same cardinal as $|K|$.

```
$\mathbf{CardOrd[n\_, k\_]}$ : $Module[\{remainder = k, m = 0, bin, t = n\},$
    $While[m <= t,$
        $bin = Binomial[t, m];$
        $If[remainder > bin,$
            $remainder -= bin,$
            $Break[]$
        $];$
        $m++$
    $];$
    $\{m, remainder\}$
$];$
```

**Algorithm 2:** CardOrd Algorithm

**Example 2.3.** *Given a set $X = \{1,2,3\}$. The class ordering of all subsets of $A$ is as follows:*

$$\emptyset \leq \{1\} \leq \{2\} \leq \{3\} \leq \{1,2\} \leq \{1,3\} \leq \{2,3\} \leq \{1,2,3\}.$$

*When we run the function CardOrd[3,7], it produces output {2,3}. The first component of the output gives the cardinal of the 7th subset $B$ of a $A$ set with the cardinal 3. The second one gives the class ordering number of $B$ in the set of the subsets of the $A$ set which has same cardinal as the that of the set $B$. Indeed, the 7th subset of a $X$ is the set $\{2,3\}$, the cardinal of the set $\{2,3\}$ is 2. Also, the subsets of the $X$ set which has same cardinal as the that of the set $\{2,3\}$ are $\{1,2\},\{1,3\},\{2,3\}$ and $\{1,2,3\}$, and the class ordering number the set of $\{2,3\}$ in the set $\{\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$ is 3. Thus, we say that the function CardOrd is working correctly.*

2.3. **Subset Algorithm.** The algorithm in Algorithm 3 giving the $k$-th subset of a set $K$ by the class ordering in $K$ is as follows:

```
$\mathbf{Subset[K\_, k\_]}$ : $Module[$
    $\{subset = \{\ \}, p, t, i, rank, ptemp, rankofelement, A = K, n, bin\},$
    $n = Length[K]; \{p, t\} = CardOrd[n, k];$
    $rank = t; ptemp = p; rankofelement = 1;$
    $For[i = 1, i <= p, i++,$
        $n--; ptemp--;$
        $While[n >= ptemp,$
            $bin = Binomial[n, ptemp];$
            $If[rank > bin,$
                $rank -= bin; n--; rankofelement++,$
                $AppendTo[subset, A[[rankofelement]]];$
                $rankofelement++; Break[]$
            $];$
        $];$
    $];$
    $subset$
$];$
```

**Algorithm 3:** Subset Algorithm

**Example 2.4.** *Given a set $A = \{3,8,5,12,9\}$. In order to get the 23rd subset of $A$, we run the function $Subset[A, 23]$ and get the output $\{8,5,12\}$.*

2.4. **Subbase Algorithm.** The task of the algorithm in Algorithm 4 is to give the $k$-th subbase which consists of subsets of a set $K$, or equivalently, to give the $k$-th subset of the power set of $K$.

```
Subbase[K_, k_] : Module[
    {subbase = { }, p, t, i, rank, ntemp, ptemp, rankofelement, bin, n},
    n = Length[K]; {p, t} = CardOrd[2^n, k];
    rank = t; ntemp = 2^n; ptemp = p; rankofelement = 1;
    For[i = 1, i <= p, i + +,
        ntemp − −; ptemp − −;
        While[ntemp ≥ ptemp,
            bin = Binomial[ntemp, ptemp];
            If[rank > bin,
                rank − = bin; ntemp −−; rankofelement ++,
                AppendTo [subbase, Subset [K, rankofelement]] ;
                rankofelement ++; Break[]
            ];
        ];
    ];
    subbase
];
```

**Algorithm 4:** Subbase Algorithm

**Example 2.5.** *Given a set* $A = \{1, 2, 3, 4\}$*. To give a topology on* $A$*, there exist* $2^{2^{|A|}} = 2^{2^4} = 65536$ *subbases to be chosen which consists of some subsets of* $A$*. If we run the function* Subbase$[A, 30000]$*, then it gives as output*

$$\{\{\,\}, \{2\}, \{3\}, \{1, 3\}, \{1, 2, 3\}, \{1, 2, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}.$$

2.5. **Base Algorithm.** The algorithm to give the set of all intersections of all sets in a finite class $K$ is given in Algorithm 5.

```
RecIntersection[K_] : Module[
    {i, j, intersection, newsets = { }, length},
    length = Length[K];
    For[i = 1, i ≤ length − 1, i ++,
        For[j = i + 1, j ≤ length, j ++,
            intersection = Intersection[K[[i]], K[[j]]];
            If[!(MemberQ[K, intersection]||MemberQ[newsets, intersection]),
                AppendTo[newsets, intersection]
            ];
        ];
    ];
    If[Length[newsets] > 1,
        newsets = Union[newsets, RecIntersection[newsets]]
    ];
    Union[K, newsets]
];
```

**Algorithm 5:** RecIntersection Algorithm

The algorithm to give as output the base induced by the $k$-th subbase consisting of some subsets of a set $K$ by class ordering in $P(K)$ is given in Algorithm 6.

```
**Base**[$\mathbf{K}\_, \mathbf{k}\_$] : $Module[\{base = \{\,\} subbase = Subbase[K, k]\},$
    $base = RecIntersection[subbase];$
    $If[!MemberQ[base, K],$
        $AppendTo[base, K]$
    $];$
    $Sort[base, ClassOrdering]$
$];$
```

**Algorithm 6:** Base Algorithm

**Example 2.6.** *Given a set $A = \{1, 2, 3, 4\}$. To give a base induced by the 2315th subbase given below on $A$,*

$$\{\{1, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}\}$$

*we run the function $Base[A, 2315]$ and then it produces as output*

$$\{\{\,\}, \{1\}, \{3\}, \{4\}, \{1, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3, 4\}\}.$$

2.6. **Topology Algorithm.** The algorithm to give the set of all unions of all sets in a finite class $K$ is given in Algorithm 7.

```
**RecUnion**[$\mathbf{K}\_$] : $Module[$
    $\{i, j, union, newsets = \{\,\}, length\},$
    $length = Length[K];$
    $For[i = 1, i \leq length - 1, i{+}{+},$
        $For[j = i + 1, j \leq length, j{+}{+},$
            $union = Union[K[[i]], K[[j]]];$
            $If[!(MemberQ[K, union] || MemberQ[newsets, union]),$
                $AppendTo[newsets, union]$
            $];$
        $];$
    $];$
    $If[Length[newsets] > 1,$
        $newsets = Union[newsets, RecUnion[newsets]]$
    $];$
    $Union[K, newsets]$
$];$
```

**Algorithm 7:** RecUnion Algorithm

The algorithm to give as output the topology induced by the $k$-th subbase consisting of some subsets of a set $K$ by class ordering in $P(K)$ is given in Algorithm 8.

**Example 2.7.** *Given a set $A = \{1, 2, 3, 4\}$. To give a topology induced by the subbase given in Example 2.6, we run the function $Topology[A, 2315]$ and get as output the topology on $A$ as follows*

$$\{\{\,\}, \{1\}, \{3\}, \{4\}, \{1, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}.$$

```
$\mathbf{Topology[K\_, k\_]} : Module[\{topology = \{\ \} base = Base[K, k]\},$
    $topology = RecUnion[base];$
    $If[!MemberQ[topology, \{\ \}],$
        $AppendTo[topology, \{\ \}]$
    $];$
    $Sort[topology, ClassOrdering]$
$];$
```

**Algorithm 8:** Topology Algorithm

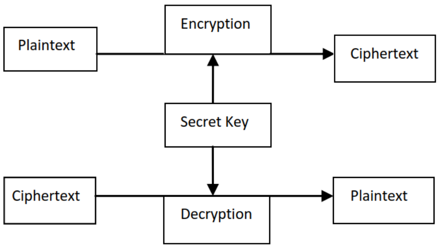

Figure 1. Alice and Bob's communication diagram

## 3. Key agreement method

We assume that Alice and Bob need a secret key as in Figure 3 in order to communicate each other cryptically.

For a secret key agreement, Alice and Bob follow their own steps in Table 3 which includes several steps of the Diffie-Hellman algorithm.

| **Step** | **Alice** | **Bob** |
|---|---|---|
| **1** | Set a set of $K_A$ of integers secretly. | Set a set of $K_B$ of integers secretly. |
| **2** | In order to get a topology on $K_A$, determine an positive integer $n_A$ as the class ordering number of subbase to be chosen. | In order to get a topology on $K_B$, determine an positive integer $n_B$ as the class ordering number of subbase to be chosen. |
| **3** | Set $\tau_A$ by assigning the output of the function $Topology[K_A, n_A]$. | Set $\tau_B$ by assigning the output of the function $Topology[K_B, n_B]$. |
| **4** | Set $\mathcal{J}_A$ by assigning the list in which it is concatenated all elements of $\tau_A$ by running the function $Join@@\tau_A$. | Set $\mathcal{J}_B$ by assigning the list in which it is concatenated all elements of $\tau_B$ by running the function $Join@@\tau_B$. |
| **5** | They specify an arbitrary positive integer $l$as public. | |
| **6** | Set $\mathcal{J}_A^*$ such that $\lvert\mathcal{J}_A^*\rvert = l$ by assigning the output of the function $PadRight[\mathcal{J}_A, l, \mathcal{J}_A]$. | Set $\mathcal{J}_B^*$ such that $\lvert\mathcal{J}_B^*\rvert = l$ by assigning the output of the function $PadRight[\mathcal{J}_B, l, \mathcal{J}_B]$. |
| **7** | They specify two arbitrary positive integers $p$ and $n$ as public. | |
| **8** | Set $\mathcal{M}_A$ by assigning the output of the function $Mod[p^{\#}, n]\&/@\mathcal{J}_A^*$, and send it to Bob as public. | Set $\mathcal{M}_B$ by assigning the output of the function $Mod[p^{\#}, n]\&/@\mathcal{J}_B^*$, and send it to Alice as public. |
| **9** | Generate the secret key $K$ by running the function $K = FromDigits/@Thread\left[Mod\left[\#1^{\#2}, n\right] \& \left[\mathcal{M}_B, \mathcal{J}_A^*\right]\right].$ | Generate the secret key $K$ by running the function $K = FromDigits/@Thread\left[Mod\left[\#1^{\#2}, n\right] \& \left[\mathcal{M}_A, \mathcal{J}_B^*\right]\right].$ |

Table 1. Key agreement method

Let's examine these steps in the key agreement method on an application.

Alice and Bob set $K_A = \{3, 7, 12, 16\}$ and $K_B = \{2, 6, 7\}$, respectively.

$n_A$ ($n_B$) denotes the class ordering number of a subbase by which a topology on the $K_A$ ($K_B$) is induced. Each subbase by which a topology on the $K_A$ ($K_B$) is induced is also an element of the power set of the power set of the $K_A$ ($K_B$). Therefore, there are $2^{2^{|K_A|}} = 2^{2^4} = 65536$ ($2^{2^{|K_B|}} = 2^{2^3} = 256$) different subbases by which a topology on $K_A$ ($K_B$) can be selected. Accordingly, $n_A$ takes a value between 1 and 65536 while $n_B$ takes a value between 1 and 256. Alice sets secretly $n_A = 40000$ while Bob sets $n_B = 200$.

The topology that Alice gets

$$\begin{gathered}\{\{\ \}, \{3\}, \{7\}, \{12\}, \{16\}, \{3, 7\}, \{3, 12\}, \{3, 16\}, \{7, 12\}, \{7, 16\}, \{12, 16\}, \\ \{3, 7, 12\}, \{3, 7, 16\}, \{3, 12, 16\}, \{7, 12, 16\}, \{3, 7, 12, 16\}\}\end{gathered}$$

while the topology that Bob gets

$$\{\{\ \}, \{2\}, \{6\}, \{7\}, \{2, 6\}, \{2, 7\}, \{6, 7\}\{2, 6, 7\}\}.$$

In this step where the open sets in each topology are concatenated, Alice and Bob set the lists

$$\begin{aligned}\mathcal{J}_A = \{&3, 7, 12, 16, 3, 7, 3, 12, 3, 16, 7, 12, 7, 16, 12, 16, \\ &3, 7, 12, 3, 7, 16, 3, 12, 16, 7, 12, 16, 3, 7, 12, 16\}, \\ \mathcal{J}_B = \{&2, 6, 7, 2, 6, 2, 7, 6, 7, 2, 6, 7\},\end{aligned}$$

respectively.

Then the number $l$ determined by Alice as 75 is sended to Bob as public. It is an arbitrary choice that the number $l$ is determined by Alice. It can also be determined by Bob. As a third way, the number $l$ can be determined as the product of two positive integers determined by Alice and Bob.

The rule of obtaining new lists is given as follows: If the cardinal of the list $\mathcal{J}_A$ ($\mathcal{J}_B$) is larger than $l$, the new list $\mathcal{J}_A^*$ ($\mathcal{J}_B^*$) consists of the first $l$ elements of that list; otherwise, each of elements of the list $\mathcal{J}_A$ ($\mathcal{J}_B$) is added to the right of the new list $\mathcal{J}_A^*$ ($\mathcal{J}_B^*$) repeatedly until $|\mathcal{J}_A^*| = l$ ($|\mathcal{J}_B^*| = l$). Then, from the list $\mathcal{J}_A$, Alice obtains new list

$$\begin{aligned}\mathcal{J}_A = \{&3, 7, 12, 16, 3, 7, 3, 12, 3, 16, 7, 12, 7, 16, 12, 16, 3, 7, 12, 3, 7, 16, 3, 12, 16, 7, 12, \\ &16, 3, 7, 12, 16, 3, 7, 12, 16, 3, 7, 3, 12, 3, 16, 7, 12, 7, 16, 12, 16, 3, 7, 12, 3, 7, 16, \\ &3, 12, 16, 7, 12, 16, 3, 7, 12, 16, 3, 7, 12, 16, 3, 7, 3, 12, 3, 16, 7\}\end{aligned}$$

while Bob obtains the new list from $\mathcal{J}_B$ as follows

$$\begin{aligned}\mathcal{J}_B^* = \{&2, 6, 7, 2, 6, 2, 7, 6, 7, 2, 6, 7, 2, 6, 7, 2, 6, 2, 7, 6, 7, 2, 6, 7, 2, 6, 7, 2, 6, 2, 7, 6, 7, 2, \\ &6, 7, 2, 6, 7, 2, 6, 2, 7, 6, 7, 2, 6, 7, 2, 6, 7, 2, 6, 2, 7, 6, 7, 2, 6, 7, 2, 6, 7, 2, 6, 2, 7, 6, \\ &7, 2, 6, 7, 2, 6, 7\}.\end{aligned}$$

As seen, the cardinal of both lists is same, that is 75.

Two positive integers $p$ and $n$ as 3 and 65, respectively, determined by Alice is sended to Bob as public. It is also an arbitrary who determines the numbers $p$ and $q$.

Alice obtains the list $\mathcal{M}_A$ defined by $\{p^{j_A} mod\, n | j_A \in \mathcal{J}_A^*\}$ as follows

$$\begin{aligned}\mathcal{M}_A = \{&27, 42, 1, 16, 27, 42, 27, 1, 27, 16, 42, 1, 42, 16, 1, 16, 27, 42, 1, 27, 42, 16, 27, 1, 16, \\ &42, 1, 16, 27, 42, 1, 16, 27, 42, 1, 16, 27, 42, 27, 1, 27, 16, 42, 1, 42, 16, 1, 16, 27, 42, \\ &1, 27, 42, 16, 27, 1, 16, 42, 1, 16, 27, 42, 1, 16, 27, 42, 1, 16, 27, 42, 27, 1, 27, 16, 42\}\end{aligned}$$

while Bob obtains the list $\mathcal{M}_B$ defined by $\{p^{j_B} mod\, n | j_B \in \mathcal{J}_B^*\}$ as follows

$$\begin{aligned}\mathcal{M}_B = \{&9, 14, 42, 9, 14, 9, 42, 14, 42, 9, 14, 42, 9, 14, 42, 9, 14, 9, 42, 14, 42, 9, 14, 42, 9, \\ &14, 42, 9, 14, 9, 42, 14, 42, 9, 14, 42, 9, 14, 42, 9, 14, 9, 42, 14, 42, 9, 14, 42, 9, 14, \\ &42, 9, 14, 9, 42, 14, 42, 9, 14, 42, 9, 14, 42, 9, 14, 9, 42, 14, 42, 9, 14, 42, 9, 14, 42\}.\end{aligned}$$

In the last step, Alice gets the the list defined by

$$\{(m_B)^{j_A}\, mod\, n | m_B \in \mathcal{M}_B, j_A \in \mathcal{J}_A^*\}$$

as follows

$$\{14, 14, 1, 61, 14, 9, 53, 1, 53, 61, 14, 1, 9, 1, 1, 61, 14, 9, 1, 14, 3, 61, 14, 1, 61, 14, 1, 61, 14, 9, 1, 1, 53, 9, 1, 16, 14, 14, 53, 1, 14, 61, 3, 1, 3, 61, 1, 16, 14, 14, 1, 14, 14, 61, 53, 1, 16, 9, 1, 16, 14, 14, 1, 61, 14, 9, 1, 1, 53, 9, 14, 1, 14, 1, 3\}$$

and generates the secret key

1547254369241917249249247247249163927593301319127542606326927547249164042413

by constructing the number in base-10 from elements of that list while Bob gets the list defined by

$$\{(m_A)^{j_B}\, mod\, n | m_A \in \mathcal{M}_A, j_B \in \mathcal{J}_B^*\}$$

as follows

$$\{14, 14, 1, 61, 14, 9, 53, 1, 53, 61, 14, 1, 9, 1, 1, 61, 14, 9, 1, 14, 3, 61, 14, 1, 61, 14, 1, 61, 14, 9, 1, 1, 53, 9, 1, 16, 14, 14, 53, 1, 14, 61, 3, 1, 3, 61, 1, 16, 14, 14, 1, 14, 14, 61, 53, 1, 16, 9, 1, 16, 14, 14, 1, 61, 14, 9, 1, 1, 53, 9, 14, 1, 14, 1, 3\}$$

and generates the secret key

1547254369241917249249247247249163927593301319127542606326927547249164042413

by constructing the number in base-10 from elements of that list. As seen, Alice and Bob share a secret key.

## References

[1] Adams, C. C. and Franzosa, R. D., (2008), Introduction to topology: pure and applied (No. Sirsi) i9780131848696). Pearson Prentice Hall Upper Saddle River.

[2] Diffie, W. and Hellman, M., (1976), New directions in cryptography. IEEE transactions on Information Theory, 22 (6), 644654.

[3] Hoffstein, J., Pipher, J. C., Silverman, J. H. and Silverman, J. H., (2008), An introduction to mathematical cryptography (Vol. 1). Springer.

[4] Munkres, J. R., (2000), Topology. Prentice Hall.

[5] Rosen, K., (2008), An introduction to cryptography, by taylor & francis group. LLC.

**Kadirhan Polat** was born in 1985, in Erzurum, Turkey. He started his undergraduate studies at Department of Mathematics, Faculty of Science, Atatürk University and graduated in 2006. He started his graduate education in 2007 at Institute of Science, Atatürk University. He completed his master's degree in 2010 and started to work as a research assistant at Ağrı İbrahim Çeçen University. He started his doctorate education in 2011 at Institute of Science, Ataturk University and completed it in 2015. He started to work as Assistant Professor at Ağrı İbrahim Çeçen University in 2015 and still continues to work at this university.