Filomat 32:19 (2018), 6519–6530
https://doi.org/10.2298/FIL1819519A

Published by Faculty of Sciences and Mathematics,
University of Niš, Serbia
Available at: http://www.pmf.ni.ac.rs/filomat

# Soft Matrix Product and Soft Cryptosystem

**Emin Aygün**[a]

[a] *Department of Mathematics, Erciyes University, 38080 Kayseri, Turkey*

**Abstract.** Soft set theory, proposed by Molodtsov, has been regarded as an effective mathematical tool to deal with uncertainties. In this work, we define two new operations on the set of soft matrices, called inverse production and characteristic production and give their properties. We introduce soft cryptosystem as a new cryptosystem method by using inverse production and characteristic production of soft matrices. We finally define soft encryption and soft decryption. Some applications are given

## 1. Introduction

The volume and complexity of the collected data in our modern society has been growing rapidly. There existed various types of uncertainties in those data related to complex problems in biology, economics, ecology, engineering, environmental science, medical science, social science, and many other fields. In order to describe and extract the useful information hidden in uncertain data, researchers in mathematics, computer science and related areas have proposed a number of theories such as probability theory, fuzzy set theory [33], intuitionistic fuzzy set theory [5,6,34], rough set theory [22] and interval mathematics [21]. While all these theories were well-known and useful approaches to describing uncertainties, each of them has its inherent difficulties as pointed out by Molodtsov [18].

In 1999, Molodtsov [18] proposed soft set theory as a new mathematical tool to deal with uncertainties which are free from the difficulties affecting existing methods. As reported in [18-20], a wide range of applications of soft sets have been developed many different fields, including the smoothness of functions, game theory, operations research, Riemann integration, Perron integration, probability theory and measurement theory. There has been a rapid growth of interest in soft set theory and its application in recent years.

By using the rough sets [22], Maji et al. [14,16] presented an application of soft sets in a decision making problem and published a detailed theoretical study on soft sets. Chen et al. [7,8] and Kong et al. [12] introduced a new definition of soft set parameterization reduction. Xiao et al. [30] and Pei and Miao [23] discussed the relationship between soft sets and information systems. Mushrif et al. [21] presented a new algorithm for the classification of natural textures. The proposed classification algorithm is based on the notions of soft set theory.

The algebraic structure of soft set theories has been studied increasingly in recent years. Aktas and Cagman [1] gave a definition of soft groups. Jun [11] introduced the Notion of soft BCK/BCI-algebras and soft subalgebras. Feng et a. [10] initiated a study of soft semirings by using the soft set theory and

2010 *Mathematics Subject Classification*. 03G25 ; 94A60; 11T71
*Keywords*. Soft sets, Soft matrix, Soft matrix product, Cyrptosystem, Soft cryptosystem
Received: 25 April 2014; Accepted: 12 August 2018
Communicated by Dragan S. Djordjević
*Email address:* eaygun@erciyes.edu.tr (Emin Aygün)

investigated several related properties. Sun et al. [29] introduced a basic version of soft sets. These approaches presented in [30] are preferable for reflecting actual states of imcomplate data in soft sets. Cagman and Enginoglu [9] defined and studied soft matrix theory. Atagun and Sezgin [4] studied on soft set operations with many corresponding examples as well. Sezgin, Atagun and Aygun [27] studied soft near-rings and idealistic soft near-rings.

Maji et al. [15] defined the fuzzy soft sets. Afterwards, many researchers have worked on this consept. Aktas and Cagman [1,2] also compared soft sets to the related concepts of fuzzy sets and rough sets, providing examples to clarify their differences. Roy and Maji [25] presented some results on an application of fuzzy soft sets in decision making problems. Yang et al. [32] defined the reduction of fuzzy soft sets and then analyzed a decision making problem by fuzzy soft sets. Majumdar and Samanta [17] introduced several similarity measures of fuzzy soft sets. Kong et al. [12] and Xiao et al. [30] presented a working of some approximations based on soft sets.

Based on theory of soft sets the analysis was developed in [30,31], and the notions of soft number, soft derivative, soft integral, etc. are formulated. This technique is applied to soft optimization problems by Kovkov et al. [13]. Based on the analysis of several operations on soft sets introduced by Ali et al. [3]. Cagman and Enginoglu [9] redefined the operations of Molodtsovs soft sets to make them more functional for improving several new results. By using these new definitions, they construct soft decision making methods.

Secret of communication is clearly one of the most important goal of cryptography, therefore many secret-key and public-key cryptosystems have been proposed to solve it. It is furthermore widely admitted that the main security notion to achieved is the semantic security [24,28] (a.k.a indistinguishability of ciphertexts). Actually, a semantically secure public-key cryptosystem is not only important for secret communications, but it is also a fundamental primitive for many more complex protocols such as electronic voting, electronic auctions and secret evaluation of functions to cite some of them. However, having a secure cryptosystem is in general not sufficient to construct efficient, solution for the above mentioned problems. In general more specific properties, such as kind of malleability, or even homomorphic relations, are very useful to obtain practical constructions.

Roughly speaking, a public-key encryption scheme allows someone to encrypt a message for a unique recipient, the one who owns the corresponding private key (a.k.a. decryption key). But in practice, there is often a natural hierarchy, either for security or for safety reasons: the head of a group may want to be able to read any message sent to the members of the group, people may want to be able to recover the plaintexts even if they loose their private key. Therefore, it is highly desirable to provide schemes that enable to deal with intermediate scenarios, in which users are allowed to process their own data, but not those of other users.

Moreover, in practice, there are many situations on which we need more than a plain an encryption function. In particular, it is often useful two have a provably secure encryption primitive that allows to perform some computation on the plaintexts without revealing them explicitly.

Up to the present, the applications of soft set theory generally solve problems with the help of the rough sets or fuzzy soft sets. In this paper, we first define soft matrices which are representations of soft sets. This representation has several advantages . It is easy to store and manipulate matrices and hence the soft sets represented by them in a computer.

The presentation of the rest of this paper is organized as follows: In the next section, we define soft matrices and give their operations. In section 3, we define inverse product, characteristic product of soft matrices and their properties. In section 4, we define soft encryption and soft decryption. In the final section, we give an example which shows that these methods successfully work.

## 2. Preliminaries

In this section we define soft matrices which are representative of the soft sets. This style of representation is useful for storing a soft set in computer memory. The operation can be presented by the matrices which are very useful and applicable.

**Definition 2.1.** *Let $U$ be an initial universe, $P(U)$ be the power set of $U$, $E$ be the set of all parameters and $A \subseteq E$. A soft set $(f_A, E)$ on the universe $U$ is defined by the set of ordered pairs*

$$(f_A, E) = \{(e, f_A(e)) : e \in E, f_A(e) \in P(U)\}$$

*where*

$$f_A : E \longrightarrow P(U)$$

*such that $f_A(e) = \emptyset$ if $e \notin A$ ([25]).*

Here, $f_A$ is called an approximate function of the soft set $(f_A, E)$. The set $f_A(e)$ is called e-approximate value set or e-approximate set which consists of related objects of the parameter $e \in E$.

**Definition 2.2.** *Let $(f_A, E)$ be a soft set over $U$. Then a subset of UxE is uniquely defined by*

$$R_A = \{(u, e) : e \in A, u \in f_A(e)\}$$

*which is called a relation form of $(f_A, E)$. The characteristic function of $R_A$ is written by*

$$\chi_{R_A} : U \times E \to \{0, 1\}, \chi_{R_A}(u, e) = \begin{cases} 1, & (u, e) \in R_A \\ 0, & (u, e) \notin R_A. \end{cases}$$

*If $U = \{u_1, u_2, ..., u_m\}$, $E = \{e_1, e_2, ..., e_n\}$, $A \subseteq E$ and*

$$a_{ij} = \chi_{R_A}(u_i, e_j)$$

*then,*

$$\left[a_{ij}\right]_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} & ... & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & ... & a_{mn} \end{bmatrix}$$

*which is called an $m \times n$ soft matrix of the soft set $(f_A, E)$ over $U$ ([11]).*

According to this definition, a soft set $(f_A, E)$ is uniquely characterized by the matrix $\left[a_{ij}\right]_{m\times n}$. It means that a soft set $(f_A, E)$ is formally equal to its soft matrix $\left[a_{ij}\right]_{m\times n}$. Therefore, we shall identify any soft set with its soft matrix and use these two concepts as interchangeable.

The set of all $m \times n$ soft matrices over $U$ will be denoted by $SM_{m\times n}$. From now we shall delete the subscripts $m \times n$ of $\left[a_{ij}\right]_{m\times n}$, we use $\left[a_{ij}\right]$ instead of $\left[a_{ij}\right]_{m\times n}$, since $\left[a_{ij}\right] \in SM_{m\times n}$ means that $\left[a_{ij}\right]$ is an $m \times n$ soft matrix for $i = 1, 2, , n$ and $j = 1, 2, , m$

**Example 2.3.** *Assume that $U = \{u_1, u_2, u_3, u_4, u_5\}$ is an universal set and $E = \{e_1, e_2, e_3, e_4\}$ is a set of all parameters. If $A = \{e_1, e_2, e_4\}$ and*
*$f_A(e_1) = \{u_2, u_3, u_4\}$, $f_A(e_2) = \{u_1, u_3, u_5\}$, $f_A(e_4) = \{u_2, u_4, u_5\}$, then we write a soft set*

$$(f_A, E) = \{(e_1, \{u_2, u_3, u_4\}), (e_2, \{u_1, u_3, u_5\}), (e_4, \{u_2, u_4, u_5\})\}$$

*and then the relation form of $(f_A, E)$ is written by*

$$R_A = \{(u_2, e_1), (u_3, e_1), (u_4, e_1), (u_1, e_2), (u_3, e_2), (u_5, e_2), (u_2, e_4), (u_4, e_4), (u_5, e_4)\}.$$

*Hence, the soft matrix $\left[a_{ij}\right]$ is written by*

$$\left[a_{ij}\right] = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

**Definition 2.4.** *Let* $\left[a_{ij}\right] \in SM_{m\times n}$. *Then* $\left[a_{ij}\right]$ *is called*

$i_1$) *a zero soft matrix, denoted by [0], if* $a_{ij} = 0$ *for all i and j,*

$i_2$) *an A-universal soft matrix, denoted by* $\left[\bar{a}_{ij}\right]$, *if* $a_{ij} = 1$ *for all* $j \in I_A = \{j : e_j \in A\}$ *and i,*

$i_3$) *a universal soft matrix, denoted by [1], if* $a_{ij} = 1$ *for all i and j ([11]).*

**Definition 2.5.** *Let* $\left[a_{ij}\right], \left[b_{ij}\right] \in SM_{m\times n}$. *Then the soft matrix* $\left[c_{ij}\right]$ *is called*

$i_1$) *union of* $\left[a_{ij}\right]$ *and* $\left[b_{ij}\right]$, *denoted* $\left[a_{ij}\right] \tilde{\cup} \left[b_{ij}\right] = \left[c_{ij}\right]$, *if* $c_{ij}$=max$\{a_{ij}, b_{ij}\}$ *for all i and j,*

$i_2$) *intersection of* $\left[a_{ij}\right]$ *and* $\left[b_{ij}\right]$, *denoted* $\left[a_{ij}\right] \tilde{\cap} \left[b_{ij}\right] = \left[c_{ij}\right]$, *if* $c_{ij}$=min$\{a_{ij}, b_{ij}\}$ *for all i and j,*

$i_3$) *complement of* $\left[a_{ij}\right]$, *denoted by* $\left[a_{ij}\right]^{\circ} = \left[c_{ij}\right]$, *if* $c_{ij} = 1 - a_{ij}$ *for all i and j ([11]).*

**Proposition 2.6.** *Let* $\left[a_{ij}\right], \left[b_{ij}\right]$ *and* $\left[c_{ij}\right] \in SM_{m\times n}$. *Then*

$i_1$) $\left[a_{ij}\right] \tilde{\cap} \left[a_{ij}\right] = \left[a_{ij}\right]$,

$i_2$) $\left[a_{ij}\right] \tilde{\cap} [0] = [0]$,

$i_3$) $\left[a_{ij}\right] \tilde{\cap} [1] = \left[a_{ij}\right]$,

$i_4$) $\left[a_{ij}\right] \tilde{\cap} \left[a_{ij}\right]^{\circ} = [0]$,

$i_5$) $\left[a_{ij}\right] \tilde{\cap} \left[b_{ij}\right] = \left[b_{ij}\right] \tilde{\cap} \left[a_{ij}\right]$,

$i_6$) $\left(\left[a_{ij}\right] \tilde{\cap} \left[b_{ij}\right]\right) \tilde{\cap} \left[c_{ij}\right] = \left[a_{ij}\right] \tilde{\cap} \left(\left[b_{ij}\right] \tilde{\cap} \left[c_{ij}\right]\right)$ *([11]).*

From the other side, for these cryptosystem, the letters of the alphabet are assigned numbers as follows:

| LETTER | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| NUMBER | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| | Q | R | S | T | U | V | W | X | Y | Z | C | G | I | O | S | U |
| | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |

Note that we start with A=0, so U is letter number 31. If each letter to binary system;

| LETTER | A | B | C | D | E | ... | S | U |
|---|---|---|---|---|---|---|---|---|
| BINARY SYSTEM | 00000 | 00001 | 00010 | 00011 | 00100 | ... | 11110 | 11111 |

where because of binary system, we have added the six letters: C, G, I, O, S, U.

## 3. Soft matrix product

In this section, we define inverse product, characteristic product of soft matrices and give their properties.

**Definition 3.1.** *Let* $\left[a_{ij}\right], \left[b_{ij}\right] \in SM_{m\times n}$. *The inverse product "*$\cdot_i$*" of* $\left[a_{ij}\right]$ *and* $\left[b_{ij}\right]$ *is defined as* $\left[a_{ij}\right] \cdot_i \left[b_{ij}\right] = \left[c_{ij}\right]$, *where* $c_{ij} = \begin{cases} 1, & if\ a_{ij} \neq b_{ij} \\ 0, & if\ a_{ij} = b_{ij} \end{cases}$ *for all i, j.*

**Example 3.2.** *Let* $U = \{u_1, u_2, u_3, u_4\}$ *be an universal set and* $E = \{e_1, e_2, e_3\}$ *is a set of parameters,* $A = \{e_1, e_2\}$ *and* $B = \{e_2, e_3\}$. *Let the soft sets* $(f_A, E) = \{(e_1, \{u_1, u_3\}), (e_2, \{u_2, u_3, u_4\})\}$, $(f_B, E) = \{(e_2, \{u_1, u_2, u_3\}), (e_3, \{u_2, u_4\})\}$ *and these corresponding soft matrices*

$$\left[a_{ij}\right] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ and } \left[b_{ij}\right] = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

*Then, their inverse product is a soft matrices*

$$\left[a_{ij}\right] ._i \left[b_{ij}\right] = \left[c_{ij}\right] = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \in SM_{4x3}.$$

**Remark 3.3.** *Since the product "$\cdot_i$" works on corresponding elements of soft matrices $[a_{ij}]$ and $[b_{ij}]$, we give following proofs by taking the product "$\cdot_i$" on the elements, considering all situations.*

**Proposition 3.4.** *The product "$\cdot_i$" is an associative operation in $SM_{m\times n}$.*

*Proof.* Since,

$$\begin{aligned}
&0\cdot_i (0\cdot_i 0) = (0\cdot_i 0)\cdot_i 0 = 0,\\
&0\cdot_i (0\cdot_i 1) = (0\cdot_i 0)\cdot_i 1 = 1,\\
&0\cdot_i (1\cdot_i 0) = (0\cdot_i 1)\cdot_i 0 = 1,\\
&0\cdot_i (1\cdot_i 1) = (0\cdot_i 1)\cdot_i 1 = 0,\\
&1\cdot_i (0\cdot_i 0) = (1\cdot_i 0)\cdot_i 0 = 1,\\
&1\cdot_i (1\cdot_i 0) = (1\cdot_i 1)\cdot_i 0 = 0,\\
&1\cdot_i (0\cdot_i 1) = (1\cdot_i 0)\cdot_i 1 = 0,\\
&1\cdot_i (1\cdot_i 1) = (1\cdot_i 1)\cdot_i 1 = 1,
\end{aligned}$$

it is obtained. □

**Proposition 3.5.** *Let $\left[a_{ij}\right] \in SM_{mxn}$. Then,*

$i_1$) $\left[a_{ij}\right] \cdot_i [0] = [0] \cdot_i \left[a_{ij}\right] = \left[a_{ij}\right]$,

$i_2$) $\left[a_{ij}\right] \cdot_i \left[a_{ij}\right] = [0]$,

$i_3$) $\left[a_{ij}\right] \cdot_i \left[a_{ij}\right]^{\circ} = [1]$,

$i_4$) $\left[a_{ij}\right] \cdot_i \left[a_{ij}\right] \cdot_i \left[a_{ij}\right] = \left[a_{ij}\right]$,

$i_5$) $\left[a_{ij}\right] \cdot_i \left[b_{ij}\right] = \left[b_{ij}\right] \cdot_i \left[a_{ij}\right]$,

$i_6$) $\left[a_{ij}\right]^{\circ} \cdot_i \left[b_{ij}\right]^{\circ} = \left[a_{ij}\right] \cdot_i \left[b_{ij}\right]$.

*Proof.* The proof is clear, hence omitted. □

**Theorem 3.6.** *The set $SM_{m\times n}$ is an abelian group with the operation "$\cdot_i$".*

*Proof.* By Proposition 3.4 and Proposition 3.5 we obtain that $(SM_{m\times n}, \cdot_i)$ is closed under "$\cdot_i$", associative, the identity is [0] and the inverse of $\left[a_{ij}\right]$ is $\left[a_{ij}\right]$. □

**Definition 3.7.** *$\left[a_{ij}\right], \left[b_{ij}\right] \in SM_{m\times n}$. The characteristic product "$\cdot_c$" of $\left[a_{ij}\right]$ and $\left[b_{ij}\right]$ is defined as $\left[a_{ij}\right] \cdot_c \left[b_{ij}\right] = \left[c_{ij}\right]$ where $c_{ij} = \begin{cases} 1, & \text{if } a_{ij} = b_{ij} \\ 0, & \text{if } a_{ij} \neq b_{ij} \end{cases}$ for all i, j.*

**Example 3.8.** *Let* $\left[a_{ij}\right], \left[b_{ij}\right] \in SM_{3\times4}$ *are be given in Example 3.2. Then, their characteristic product is a soft matrices*

$$\left[a_{ij}\right] \cdot_c \left[b_{ij}\right] = \left[c_{ij}\right] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} \in SM_{4\times3}.$$

**Proposition 3.9.** *Let* $\left[a_{ij}\right], \left[b_{ij}\right] \in SM_{m\times n}$. *Then,*

$i_1$) *The product "*$\cdot_c$*" is an associative operation in* $SM_{m\times n}$.

$i_2$) $\left[a_{ij}\right] \cdot_c [1] = \left[a_{ij}\right]$,

$i_3$) $\left[a_{ij}\right] \cdot_c [0] = \left[a_{ij}\right]^{\circ}$,

$i_4$) $\left[a_{ij}\right] \cdot_c \left[a_{ij}\right] = [1]$,

$i_5$) $\left[a_{ij}\right] \cdot_c \left[a_{ij}\right]^{\circ} = [0]$,

$i_6$) $\left[a_{ij}\right] \cdot_c \left[b_{ij}\right] = \left[b_{ij}\right] \cdot_c \left[a_{ij}\right]$,

$i_7$) $\left[a_{ij}\right]^{\circ} \cdot_c \left[b_{ij}\right]^{\circ} = \left[a_{ij}\right] \cdot_c \left[b_{ij}\right]$.

*Proof.* It is clear from Proposition 3.5 and Definition 3.7. □

**Theorem 3.10.** $(SM_{m\times n}, \cdot_i, \tilde{\cap})$ *is a commutative ring with unity.*

*Proof.*

$i_1$) By Theorem 3.6 $(SM_{m\times n}, \cdot_i)$ is an abelian group.

$i_2$) From Proposition 2.6 $(SM_{m\times n}, \tilde{\cap})$ is a semi-group.

$i_3$) Below, right and left distributive laws hold:

$$\begin{aligned}
&(0\tilde{\cap}0) \cdot_i (0\tilde{\cap}0) = (0\cdot_i 0) \tilde{\cap} 0 = 0,\\
&(0\tilde{\cap}1) \cdot_i (0\tilde{\cap}1) = (0\cdot_i 0) \tilde{\cap} 1 = 0,\\
&(0\tilde{\cap}1) \cdot_i (1\tilde{\cap}1) = (0\cdot_i 1) \tilde{\cap} 1 = 1,\\
&(1\tilde{\cap}1) \cdot_i (1\tilde{\cap}1) = (1\cdot_i 1) \tilde{\cap} 1 = 0,\\
&(0\tilde{\cap}0) \cdot_i (1\tilde{\cap}0) = (0\cdot_i 1) \tilde{\cap} 0 = 0,\\
&(1\tilde{\cap}0) \cdot_i (1\tilde{\cap}0) = (1\cdot_i 1) \tilde{\cap} 0 = 0,\\
&(1\tilde{\cap}1) \cdot_i (0\tilde{\cap}1) = (1\cdot_i 0) \tilde{\cap} 1 = 1,\\
&(1\tilde{\cap}0) \cdot_i (0\tilde{\cap}0) = (1\cdot_i 0) \tilde{\cap} 0 = 0.
\end{aligned}$$

$i_4$) By Proposition 2.6, the semi-group $(SM_{m\times n}, \tilde{\cap})$ is abelian and has a identity.
Hence $(SM_{m\times n}, \cdot_i, \tilde{\cap})$ is a commutative ring with unity. □

**Proposition 3.11.** *Let* $\left[a_{ij}\right], \left[b_{ij}\right] \in SM_{m\times n}$. *Then the following De Morgan's laws are valid*

$$\begin{aligned}
&i_1)\ \left(\left[a_{ij}\right] \cdot_i \left[b_{ij}\right]\right)^{\circ} = \left[a_{ij}\right]^{\circ} \cdot_c \left[b_{ij}\right]^{\circ}\\
&i_2)\ \left(\left[a_{ij}\right] \cdot_c \left[b_{ij}\right]\right)^{\circ} = \left[a_{ij}\right]^{\circ} \cdot_i \left[b_{ij}\right]^{\circ}.
\end{aligned}$$

*Proof.*

$i_1$) Since,

$$(0\cdot_i 0)^\circ = 0^\circ\cdot_c 0^0 = 1,$$
$$(0\cdot_i 1)^\circ = 0^\circ\cdot_c 1^0 = 0,$$
$$(1\cdot_i 0)^\circ = 1^\circ\cdot_c 0^0 = 0,$$
$$(1\cdot_i 1)^\circ = 1^\circ\cdot_c 1^0 = 1,$$

it is obtained. The rest of proof is similar, hence omitted. □

In Proposition 3.11, we showed the De Morgan's law for inverse product and characteristic product. We illustrate in Proposition 3.12 how De Morgan's type of results hold in $SM_{m\times n}$ for inverse product and characteristic product.

**Proposition 3.12.** *Let* $\left[a_{ij}\right] = A$, $\left[b_{ij}\right] = B$ *and* $\left[c_{ij}\right] = C \in SM_{m\times n}$. *Then*

$i_1$) $(A\cdot_i B)\cdot_c C = A^c\cdot_c (B\cdot_i C^c)$,

$i_2$) $(A\cdot_c B)\cdot_i C = A^c\cdot_i (B\cdot_c C^c)$,

$i_3$) $A\cdot_i (B\cdot_c C) = (A^c\cdot_c B)\cdot_i C^c$,

$i_4$) $A\cdot_c (B\cdot_i C) = (A^c\cdot_i B)\cdot_c C^c$.

*Proof.* By Proposition 3.10,

$$\begin{aligned}(A\cdot_i B)\cdot_c C &= (A^c\cdot_c B^c)\cdot_c C^c\\ &= A^c\cdot_c (B^c\cdot_c C)\\ &= A^c\cdot_c (B\cdot_i C^c).\end{aligned}$$

Hence, the proof is completed. The rest of proof is similar, therefore omitted. □

Now, we give a corresponding example of part $i_1$ of Proposition 3.12.

**Example 3.13.** *Let* $A, B, C \in SM_{4\times 5}$ *and*

$$A = \begin{bmatrix} 1 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 0 & 1\\ 0 & 0 & 1 & 1 & 0\\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}, B = \begin{bmatrix} 0 & 1 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 1\\ 1 & 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}, C = \begin{bmatrix} 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 1\\ 1 & 1 & 1 & 0 & 1\\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

*Thus,*

$$(A\cdot_i B)\cdot_c C = A^c\cdot_c (B\cdot_i C^c) = \begin{bmatrix} 1 & 0 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 0\\ 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

## 4. Soft cryptosystem

In this section, we suggest a new encryption scheme which are based on soft sets and soft matrices. We define soft encryption and soft decryption. Throughout this section, we denote a soft matrix by $S$, a message by $M$ and a cipher text by $C$.

**Theorem 4.1.** *Let* $S, M, C \in SM_{m\times n}$. *Then*

$i_1$) $S\cdot_i M = C$,

$i_2$) $S\cdot_c M = C$,

$i_3$) $(S\cdot_i M)\cdot_c S = C$,

$i_4$) $(S\cdot_c M)\cdot_i S = C^c$,

$i_5)$ $S\cdot_i (M\cdot_c S) = C^c$,

$i_6)$ $S\cdot_c (M\cdot_i S) = C$.

*Proof.* By the definitions of the inverse product and characteristic product, its can be easily obtained. □

Alice wants to send a message to Bob, but they have not had previous contact and they do not want to take the time to send a courier with a key. Therefore, all information that Alice sends to Bob will potentially be obtained by the evil observer Eve. However, it is still possible for a message to be sent in such a way that Bob can read it but Eve cannot.

With all the previously discussed methods, this would be impossible. Alice would have to send key, which Eve would intercept. She could then decrypt all subsequent messages.

The soft cryptosystem scheme is given by the following two algorithm.
Soft encryption algorithm with Theorem 4.1 ($i_1$):

1. Alice takes a soft set.

2. Alice finds corresponding soft matrix.

3. Alice parts message blocks and transfers to binary system.

4. Alice makes $\cdot_i$ – *product* message with soft matrix.

5. Alice turns from matrix to letter and sends to Bob.

Soft decryption algorithm with Theorem 4.1 ($i_1$):

1. Bob takes soft sets and soft matrix.

2. Bob parts cipher text blocks and transfers to binary system.

3. Bob makes $\cdot_i$ – *product* cipher text with soft matrix.

4. Bob turns from matrix to letter.

5. Bob obtains message.

**Remark 4.2.** *In the soft cryptosystem scheme; we don't have to separate the message into blocks. However, to separate the message into blocks may be even more difficult for long message. Therefore, we divide the messages into blocks.*

Similarly, this new cryptosystem would be applied to characteristic product with Theorem 4.1 ($i_2$):

Soft encryption algorithm with Theorem 4.1 ($i_3$):

1. Alice takes a soft set and finds corresponding soft matrix.

2. Alice parts message blocks and transfers to binary system.

3. Alice makes $\cdot_i$ –*product* from left to message with soft matrix.

4. Alice makes $\cdot_c$ $-$*product* from right to message with soft matrix.

5. Alice turns from matrix to letter and sends to Bob.

Soft decryption algorithm with Theorem 4.1 ($i_3$):

1. Bob takes soft set and soft matrix.

2. Bob parts cipher text blocks and transfers to binary system.

3. Bob makes $\cdot_c$ $-$*product* and $\cdot_i$ $-$ *product* cipher text with soft matrix, respectively.

4. Bob turns from matrix to letter.

5. Bob obtains message.

**Remark 4.3.** *This system depends on soft sets and soft matrices. Thus, in the above system makes fast encryption and decryption. To avoid attacks, we should be careful in the choice of soft sets. If we choose elements of the soft sets thus encryption security is increased. Also similarly operations of column can make which make operations with line to which our scheme can be applied. The encryption operation can be made with a single matrix without splitting into blocks. We should select 5 members of set of parameters, for we can make the following encryption.*

## 5. Applications

Soft encryption algorithm with Theorem 4.1 ($i_1$):
Alice wants to send a message to Bob. Let "SOFT ENCRYPTION" is the message.

1. Alice takes $(f_A, E) = \{(e_1, \{u_1, u_2, u_3\}), (e_2, \{u_1, u_4, u_5\}), (e_3, \{u_2, u_3\}), (e_4, \{u_4, u_5\}), (e_5, \{u_1, u_2, u_4\})\}$.

2. Alice finds a soft matrix and it is

$$S = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

3. Alice parts message blocks. "SOFTE-NCRYP-TIONA". Matrix of the message is respectively

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

4. Alice makes $\cdot_i$ $-$*product* message with soft matrix, respectively.

$$M \cdot_i S = C = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

5. Alice turns from matrix to letter. The chipper text is ”LGRYO-UXFTF-KOCGK”. She send ”LGRYO-UXFTF-KOCGK” to Bob.

Soft decryption algorithm with Theorem 4.1 ($i_1$):
1. Bob takes a soft set and a soft matrix. Soft set is

$$(f_A, E) = \{(e_1, \{u_1, u_2, u_3\}), (e_2, \{u_1, u_4, u_5\}), (e_3, \{u_2, u_3\}), (e_4, \{u_4, u_5\}), (e_5, \{u_1, u_2, u_4\})\}$$

Soft matrix is

$$S = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

2. Bob parts cipher text blocks. ”LGRYO-UXFTF-KOCGK” and transfers to binary system.

$$C = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

3. Bob makes $\cdot_i$ $-$*product* cipher text with soft matrix respectively.

$$C \cdot_i S = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

4. Bob turns from matrix to letter. ”SOFTE-NCRYP-TIONA”.
5. Bob obtains message. ”SOFT ENCRYPTION”.

Soft encryption algorithm with Theorem 4.1 ($i_3$):

Alice wants to send above message to Bob.

1. Alice takes a soft set and finds corresponding soft matrix as above.

2. Alice parts message blocks ”SOFTE-NCRYP-TIONA”. Matrix of the message is respectively

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

3. Alice makes $\cdot_i$ $-$*product* from left to message with soft matrix.

$$S \cdot_i M = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

4. Alice makes $\cdot_c$ $-product$ from left to message with soft matrix.

$$(S\cdot_i M)\cdot_c S = C\left[\begin{array}{ccccc}0&1&1&0&1\\1&0&0&0&1\\1&0&0&1&0\\0&1&1&0&0\\1&1&0&1&1\end{array}\right],\left[\begin{array}{ccccc}1&0&0&1&0\\1&1&1&0&1\\0&1&1&1&0\\0&0&1&1&1\\1&0&0&0&0\end{array}\right],\left[\begin{array}{ccccc}0&1&1&0&0\\1&0&1&1&1\\1&0&0&0&1\\1&0&1&1&0\\1&1&1&1&1\end{array}\right].$$

5. Alice turns from matrix to letter. The cipher text is "NRSMG-SOOHQ-MXRVU". She sends "NRSMG-SOOHQ-MXRVU" to Bob.

Soft decryption algorithm with Theorem 4.1 ($i_3$):

1. Bob takes a soft set and finds corresponding soft matrix as above.

2. Bob parts cipher text blocks. "NRSMG-SOOHQ-MXRVU" and transfers to binary system.

$$C=\left[\begin{array}{ccccc}0&1&1&0&1\\1&0&0&0&1\\1&0&0&1&0\\0&1&1&0&0\\1&1&0&1&1\end{array}\right],\left[\begin{array}{ccccc}1&0&0&1&0\\1&1&1&0&1\\0&1&1&1&0\\0&0&1&1&1\\1&0&0&0&0\end{array}\right],\left[\begin{array}{ccccc}0&1&1&0&0\\1&0&1&1&1\\1&0&0&0&1\\1&0&1&1&0\\1&1&1&1&1\end{array}\right].$$

3. Bob makes $\cdot_c$ $-product$and $\cdot_i$ $-$ $product$ cipher text with soft matrix, respectively.

$$C\cdot_c S=\left[\begin{array}{ccccc}0&1&0&1&1\\1&1&0&1&1\\1&0&0&0&1\\1&1&0&0&0\\0&1&1&1&0\end{array}\right],\left[\begin{array}{ccccc}1&0&1&0&0\\1&0&1&1&1\\0&0&1&0&1\\1&0&0&1&1\\0&0&1&0&1\end{array}\right],\left[\begin{array}{ccccc}0&1&0&1&0\\1&1&1&0&1\\1&1&0&1&0\\0&0&1&1&0\\1&1&0&1&0\end{array}\right].$$

$$A\cdot_i(C\cdot_c S)=\left[\begin{array}{ccccc}1&0&0&1&0\\0&1&1&1&0\\0&0&1&0&1\\1&0&0&1&1\\0&0&1&0&0\end{array}\right],\left[\begin{array}{ccccc}0&1&1&0&1\\0&0&0&1&0\\1&0&0&0&1\\1&1&0&0&0\\0&1&1&1&1\end{array}\right],\left[\begin{array}{ccccc}1&0&0&1&1\\0&1&0&0&0\\0&1&1&1&0\\0&1&1&0&1\\0&0&0&0&0\end{array}\right].$$

4. Bob turns from matrix to letter. "SOFTE-NCRYP-TIONA".
5. Bob obtains message: "SOFT ENCRYPTION".

Remark Similarly, this new cryptosystem's applications would be applied to Theorem 4.1 ($i_4$), ($i_5$) and ($i_6$).

## References


[1] H. Aktas, N. Cagman, Soft sets and soft groups. Inform Sci 177 (2007) 2726-2735.
[2] H. Aktas, N. Cagman, Erratum to "Soft sets and soft groups", Information Sciences 3 (2009), 338. Inform. Sci. 177 (2007) 2726–2735.
[3] M.I. Ali, F. Feng, X. Liu, W. K. Min, M. Shabir, On some new operations in soft set theory, Computers and Mathematics with Applications 57 (9) (2009) 1547–1553.
[4] A. O. Atagun, A. Sezgin, Soft substructures of rings, fields and modules. Comput Math Appl 61(3) (2011) 592-601.
[5] K. Atanassov, Operators over interval valued intuitionistic fuzzy sets, Fuzzy Sets and Systems 64 (1994) 159–174.
[6] K. Atanassov, Intuitionistic fuzzy sets, Fuzzy Sets and Systems 20 (1986) 87–96.
[7] D. Chen, E. C. C. Tsang, D. S. Yeung, X. Wang, The parametrization reduction of soft sets and its applications, Computers and Mathematics with Applications 44 (2002) 1077–1083.
[8] D. Chen, E. C. C. Tsang, D. S. Yeung, X. Wang, Some notes on the parameterization reduction of soft sets, International Conference on Machine Learning and Cybernetics, vol. 3 (2003) 1442–1445.
[9] N. Cagman, S. Enginoglu, Soft matrix theory and its decision making. Comput Math Appl 59 (2010) 3308-3314.

[10] F. Feng, Y. B. Jun, X. Zhao, Soft semirings. Comput Math Appl 56 (2008) 2621-2628.
[11] Y. B. Jun, Soft BCK/BCI-algebras. Comput Math Appl 56 (2008) 1408-1413.
[12] Y. B. Jun, C. H. Park, Applications of soft sets in ideal theory of BCK/BCI-algebras. Inform Sci 178 (2008) 2466-2475.
[13] Z. Kong, L. Gao, L. Wang, S. Li, The parameter reduction of soft sets and algorithm, Computers and Mathematics with Applications 56 (12) (2008) 3029–3037.
[14] D. V. Kovkov, V. M. Kolbanov, D. A. Molodtsov, Soft sets theory-based optimization, Journal of Computer and Systems Sciences International 46 (6) (2007) 872–880.
[15] P. K. Maji, R. Biswas, A. R. Roy, Soft set theory, Computers and Mathematics with Applications 45 (2003) 555–562.
[16] P. K. Maji, R. Biswas, A. R. Roy, Fuzzy soft sets, Journal of Fuzzy Mathematics 9 (3) (2001) 589–602.
[17] P. K. Maji, A. R. Roy, R. Biswas, An application of soft sets in a decision making problem, Computers and Mathematics with Applications 44 (2002) 1077–1083
[18] D. Molodtsov, Soft set theory-first results. Comput Math Appl 37 (1999) 19-31.
[19] D. Molodtsov, The description of a dependence with the help of soft sets, Journal of Computer and Systems Sciences International 40 (6) (2001) 977–984.
[20] D. Molodtsov, The Theory of Soft Sets, URSS Publishers. , Moscow,(in Russian), 2004.
[21] M.M. Mushrif, S. Sengupta, A. K. Ray, Texture classification using a novel, soft-set theory based classification, algorithm, Lecture Notes in Computer Science 3851 (2006) 246–254.
[22] Z. Pawlok, A. Skowron, Rudiments of soft sets, Information Sciences 177 (2007) 3–27.
[23] D. Pei, D. Miao, From soft sets to information systems, in: X. Hu, Q.Liu, A. Skowron, T.Y. Lin, R.R. Yager, B. Zhang (Eds.), Proceedings of Granular Computing, vol. 2, IEEE, pp. (2005) 617–621.
[24] R. Rivest, L. Adleman, M. Dertouzos, On data banks and privacy homomorphisms, In Foundations of Secure Computation, (1978) 169–180.
[25] A. R. Roy, P. K. Maji, A fuzzy soft set theoretic approach to decision making problem, Journal of Computational and Applied Mathematics 203, (2007) 412–418.
[26] A. Sezgin, A.O. Atagun, On operations of soft sets, Computers and Mathematics with Applications 61, (2011) 1457–1467.
[27] A. Sezgin, A.O. Atagun, E. Aygun, A note on soft near-rings and idealistic soft near-rings, Filomat Vol. 25, (1),(2011) 53–68.
[28] Stinson D, Cyrptography: Theory and Practice, CRC Press, New Jersey, 573pp, 1995.
[29] Q. M. Sun, Z. L. Zhang, J. Liu, A Soft sets and soft modules, in: Guoyin Wang, Tian-rui Li, Jerzy W. Grzymala-Busse, Duoqian Miao, Andrzej Skowron, Yiyu Yao (Eds.), Rough Sets and Knowledge Technology, RSKT-2008, Proceedings, Springer, pp. 403–409, 2008.
[30] Z. Xiao, L. Chen, B. Zhong, S. Ye, Recognition for soft information based on the theory of soft sets, in: J.Chen (Ed.), Proceedings of ICSSSM-05, vol. 2, IEEE, pp. (2005) 1104–1106.
[31] C. F. Yang, A note on soft set theory, Computers and Mathematics with Applications 56 (2008), 1899–1900. [Comput. Math. Appl. 45 (4-5),(2003) 555–562].
[32] X. Yang, D. Yu, J. Yang, C. Wu, Generalization of soft set theory: from crisp to fuzzy case, in: Bing-Yuan Cao (Ed.), Fuzzy Information and Engineering: Proceedings of ICFIE-2007, in: Advances in Soft Computing, vol. 40, Springer, pp. (2007) 345–355.
[33] L. A. Zadeh, Fuzzy sets, Information and Control 8 (1965) 338–353.
[34] L. Zhou, W. Wu, On generalized intuitionistic fuzzy rough approximation opeartors, Information Sciences 178 (11)(2008) 2448–2465.