JOURNAL OF INDUSTRIAL AND
MANAGEMENT OPTIMIZATION
Volume **16**, Number **4**, July **2020**

doi:10.3934/jimo.2019036

pp. **1927–1941**

AN APPLICATION OF CRYPTO CLOUD COMPUTING IN SOCIAL NETWORKS BY COOPERATIVE GAME THEORY

Serap Ergün

Department of Electrical and Electronic Engineering
Isparta University of Applied Sciences, Isparta, Turkey

Barış Bülent Kirlar and Sirma Zeynep Alparslan Gök*

Department of Mathematics, Süleyman Demirel University, Isparta, Turkey
Institute of Applied Mathematics, METU, Ankara, Turkey

Gerhard-Wilhelm Weber

Faculty of Engineering Management, Chair of Marketing and Economic Engineering
Poznan University of Technology, Poznan, Poland
Institute of Applied Mathematics, METU, Ankara, Turkey

(Communicated by Stefan Wolfgang Pickl)

Abstract. In this paper, we mathematically associate Crypto Cloud Computing, that has become an emerging research area, with Cooperative Game Theory in the presence of uncertainty. In the sequel, we retrieve data from the database of Amazon Web Service. The joint view upon Crypto Cloud Computing, Cooperative Game Theory and Uncertainty management is a novel approach. For this purpose, we construct a cooperative interval game model and apply this model to Social Networks. Then, we suggest some interval solutions related with the model by proposing a novel elliptic curve public key encryption scheme over finite fields having the property of semantic security. The paper ends with concluding words and an outlook to future studies.

1. **Introduction.** In the last decays, social networks have been a very important structure for users who are interconnecting through a variety of relations. Some popular social networking platforms are Facebook, Twitter, YouTube, etc. Social networks allow users to share information and form connections between one another, helping to improve the internet usability by storing content in cloud storage. In recent years, these kinds of interactions have been constructed towards the direction of how cryptographic tools can be employed to address a game-theoretical problem in the field of social networks (see [38]). Researchers think that Crypto Cloud Computing system can be designed so as to satisfy the needs of many users of the cloud by using game theory [1, 19, 38]. Cloud providers such as Google App Engine, Amazon EC2/S3, Microsoft Azure, Eucalyptus and Nimbus offer access into scalable virtualized resources [19].

On social network websites and cloud services, one of the magnificent concerns is the security and privacy of personal data. To control these information, being shared

2010 *Mathematics Subject Classification.* Primary: 91A12, 94A60; Secondary: 68P25.

Key words and phrases. Cooperative game theory, cloud computing, elliptic curves, social networks, uncertainty, interval solutions.

* Corresponding author: Sırma Zeynep Alparslan Gök.

with other users and social applications is too important to be denied [25]. Cloud computing security corresponds to the technology which is used for protecting data and applications of the cloud from threats like disruption of services, unauthorized access, modification, etc. [1].

In the sequel, proposing the discrete logarithm problem by the help of the group of points on an elliptic curve defined over a finite field was proposed by Miller [45] and Koblitz [39] independently, elliptic curve cryptosystems (ECC) have attracted so much interest from the community of researchers. In fact, the attractability of ECC is given because of the fact that no subexponential algorithm employed for solving discrete logarithm problem on the chosen elliptic curve and the underlying field properly. For this reason, one can benefit from an elliptic curve group which is smaller in size than in other systems such as RSA and DSA, while having the same level of security. Involving smaller key sizes result in storage space and bandwidth savings, and faster implementations. This makes ECC appropriate for constrained devices like smart cards and cellular phones.

From the advent of elliptic curve cryptosystems, many methods are proposed to accelerate the arithmetic on elliptic curves. The implication of different coordinate systems for representation of group elements and the usage of alternate forms of elliptic curves are two of them. Different coordinate systems such as projective, jacobian, inverted, etc., have been deeply studied in [11, 30]. Alternate forms of elliptic curves to the well-known Weierstrass curve can be classified in Edwards curves [9, 12, 13, 23, 31], Jacobi intersections and Jacobi quartics [14, 27, 31, 32, 42], Hessian curves [10, 26, 29, 34, 52], Huff curves [20, 22, 33, 35, 48, 55], and their variants. The group structure of these curves has been already studied in [11] because of having some nice properties such as resistance to the side-channel attacks. Applying the unified addition formula, meaning that point addition and point doubling have the same formula, provides a countermeasure to these attacks. In our work, we propose a novel public key scheme by using elliptic curves over finite fields which fulfills the property of semantic security. Furthermore, the cost of the proposed scheme varies depending on the models of elliptic curves and the type of coordinate systems.

Forming a coalition is very important and necessary for providers to prevent from low security which induces a risk for its customers [43]. This leads us to Cooperative Game Theory, where the players can possibly evoke extra gains or save costs by working together, and to share them in a fair way. One way is to study general properties of games arising from a particular type of an Operational Research (OR) problem and to apply it to a suitable game-theoretical solution. Another way is to consider a suitable allocation rule [16].

In our model, we follow an algorithm to create a minimum cost spanning tree (mcst), which is an OR situation related with a graph. After constructing an mcst, an allocation problem has to be found for minimizing total costs. This allocation problem is proposed by Claus and Kleitman [21]. Moreover, Bird [15] took into account the problem by using game theory and proposed an allocation rule, named the Bird rule. Furthermore, we consider the Shapley value [50], which is used in most of the models in cooperative game theory [2].

On the other hand, in many real-life situations, uncertainty exists and influences the values of the coalitions. Hence, cooperative game theory has been extended to different models providing decision making in situations which are characterized by including uncertainty implied. In these models, the characteristic functions are

not crisp like in the classical case. The outcome of cooperation includes uncertainty in different forms such as stochastic uncertainty, fuzzy uncertainty, interval uncertainty, ellipsoidal uncertainty, grey uncertainty, etc. [5, 28, 44, 53]. Cooperative interval games and related interval solution concepts are suitable models which give an aid to decision making in collaborative situations under uncertainty [4, 18]. The model of cooperative interval games supposes that for each coalition a lower and an upper bound of the outcome of cooperation can be forecasted, without any probabilistic assumptions [17].

In a majority of the real-life situations, players who are considering cooperation sign a contract without knowing the payoffs of the coalitions. But, with certainty they know their lower and upper bounds. These kinds of contracts are made to specify how interval uncertainty regarding the coalition values is incorporated in the allocation of the worth of the grand coalition before its uncertainty is resolved, and how the realization of payoff for the grand coalition is eventually allocated among the players [3]. An important issue which the players have to agree upon in order to construct cooperation in the grand coalition is how to transform an interval allocation into a crisp payoff when the uncertainty regarding the grand coalition's value is removed. A technique to transform an interval allocation into a payoff vector establishes a basic tool of contracts which players have to sign when they cannot assess with certainty the coalition payoffs [17].

In [38], the theory of Crypto-Cloud Computing with an efficient encryption algorithm under XTR by bringing together main topics of Cloud Computing, Cooperative Game Theory and Cryptology is introduced. The most interesting property of this work is the synergy achieved between cryptographic solutions and the cooperative game theory world in financial problems of Cloud Computing application areas. Uncertainty is a daily basis of real life. In many cases, we can not know the crisp values of the coalitions' values. Hence, we construct a model with interval costs.

In this paper, inspired by [38], we implement social networks to Crypto-Cloud Computing by constructing a cooperative game model. Here, a main novelty is to associate Crypto Cloud Computing with Cooperative Game Theory in the presence of uncertainty. In the sequel, we build the connection by retrieving data from the database of Amazon Web Service. Furthermore, we construct a cooperative interval game model and apply this model to Social Networks with this information. Moreover, we suggest some interval solutions related with the model by proposing a novel elliptic curve public key encryption scheme over finite fields having the property of semantic security.

The rest of the paper continues as follows. First, we give some preliminaries from cooperative interval games, graph theory and related solution concepts in Section 2. Section 3 introduces the elliptic curves over finite fields and proposes a novel encryption scheme that the security depends on the elliptic curve discrete logarithm problem and elliptic curve Diffie-Hellman problem. Information about Amazon Web Service and a cooperative interval game application on Social Networks with some interval solutions are stated in Section 4. Section 5 concludes with some final remarks and recommendations about future research.

2. **Preliminaries.**

In this section, mathematical background of interval calculus, game theory and graph theory is provided.

Let $I, J \in I(\mathbb{R})$ with $I = \left[\underline{I}, \overline{I}\right]$, $J = \left[\underline{J}, \overline{J}\right]$ be two intervals and $\alpha \in \mathbb{R}_+$. Here, addition is defined by $I + J = \left[\underline{I} + \underline{J}, \overline{I} + \overline{J}\right]$, and positive scalar multiplication is

given by $\alpha I = \left[\alpha \underline{I}, \alpha \overline{I}\right]$. The partial subtraction operator is written as $I - J$, only if $|I| \geq |J|$, where $|I| = \overline{I} - \underline{I}$. It means that $I - J = \left[\underline{I}, \overline{I}\right] - \left[\underline{J}, \overline{J}\right] = \left[\underline{I} - \underline{J}, \overline{I} - \overline{J}\right]$.

A cooperative interval game is an ordered pair $< N, c >$, where $N = \{1, \ldots, n\}$ stands for the set of players, $c : 2^N \to I(\mathbb{R})$ is the characteristic function such that $c(\emptyset) = [0, 0]$. Here, $I(\mathbb{R})$ is the set of all compact intervals in $\mathbb{R}$. The worth of a coalition S is defined by $c(S) = [\underline{c}(S), \overline{c}(S)]$. With IG^N we denote the set of all cooperative interval games with player set N. $I(\mathbb{R})^N$ denotes the set of all n-dimensional intervals. Some coalition values $c(S)$ may be degenerate intervals, defined by $\underline{c}(S) = \overline{c}(S)$ [18].

A minimum interval cost spanning tree situation (micst) is a situation, where $N = \{1, 2, \ldots, n\}$ is the set of players willing to be connected as cheap as possible to a source denoted by 0, based on an interval-valued cost function [46]. In an micst situation, for each player $i \in N$ the cost of the first edge on the unique path from player i to the player source constructs the Bird's tree allocation denoted by $\beta^R(T)$ [15, 16].

Consider a tuple given by $< N, \{0\}, A, \widehat{c} >$, where $N = \{1, ..., n\}$ represents the set of players, $\langle N \cup \{0\}, A\rangle$ is a rooted directed graph with $N \cup \{0\}$ as a set of vertices, $A \subset N \times (N \cup \{0\})$ as a set of arcs, and where 0 is the root. Furthermore, $\widehat{c} : A \to I(\mathbb{R}_+)$ is a nonnegative interval function defined on the set of arcs, and $\widehat{b}(k)$ of $k \in N$ is the possible best connection (for details see [24, 54]).

An interval solution concept on IG^N is a map assigning to each interval game $c \in IG^N$ a set of n-dimensional vectors whose components belong to $I(\mathbb{R})$.

In this investigation, we use the interval Bird rule as a solution concept. The interval Bird allocation (cf. [4]) is

$$IB(N, \{0\}, A, \widehat{c}) = (IB_1, IB_2, ..., IB_n) \in I(\mathbb{R})^N$$

with

$$IB_k(N, \{0\}, A, \widehat{c}) = (\widehat{w}(k, \widehat{b}(k)), \quad k = 1, 2, ..., n.$$

A game $< N, c >$ is named as size monotonic if $< N, |c| >$ is monotonic. Here, $SMIG^N$ stands for the class of size monotonic interval games with player set N. Moreover, $\Pi(N)$ is the set of permutations $\sigma : N \to N$. Let be given some $c \in SMIG^N$. The interval marginal operator corresponding to σ and the interval marginal vector of c with respect to σ are notated through m^σ and $m^\sigma(c)$, respectively. If we denote the set of predecessors of i in σ by $P_\sigma(i) = \left\{r \in N | \sigma^{-1}(r) < \sigma^{-1}(i)\right\}$, then $m^\sigma_{\sigma(k)}(c) = c(P_\sigma(\sigma(k)) \cup \{\sigma(k)\}) - c(P_\sigma(\sigma(k)))$, or $m^\sigma_i(c) = c(P_\sigma(i) \cup \{i\}) - c(P_\sigma(i))$. Here, $\sigma^{-1}(i)$ names the entrance number of player i [3].

In this study, we also involve the interval Shapley value (cf. [18]) as a solution concept. The *interval Shapley value* $\Phi : SMIG^N \to I(\mathbb{R})^N$ is defined as the combination

$$\Phi(c) = \frac{1}{n!} \sum_{\sigma \in \Pi(N)} m^\sigma(c), \text{ for each } c \in SMIG^N.$$

Now, we deal with the cooperation under interval uncertainty inside of the set of N players. The players use an interval solution concept named as Ψ, related with the associated cooperative interval game $< N, c >$. Here, an interval allocation $\Psi(c) = (J_1, \ldots, J_n) \in I(\mathbb{R})^N$ guarantees for each player $i \in N$ a payoff eventually within the interval $J_i = [\underline{J}_i, \overline{J}_i]$ if the value of the grand coalition $c(N)$ is known. Obviously, $\underline{c}(N) = \sum_{i \in N} \underline{J}_i$ and $\overline{c}(N) = \sum_{i \in N} \overline{J}_i$. For each $i \in N$ the interval $[\underline{J}_i, \overline{J}_i]$ can be seen as the interval claim of i on the realization $R \in c(N)$ of the

payoff for the grand coalition N ($\underline{c}(N) \leq R \leq \overline{c}(N)$). We determine the payoffs as $x_i \in [\underline{J}_i, \overline{J}_i]$, $i \in N$, such that $\sum_{i\in N} x_i = R$. The amount R to be divided between the players is smaller than $\sum_{i\in N} \overline{J}_i$ implying the bankruptcy rules. These rules are appropriate candidates for transforming an interval allocation $(J_1, \ldots, J_n)$ into a payoff vector $(x_1, \ldots, x_n) \in \mathbb{R}^N$ [17].

A bankruptcy situation with a set of players N means a pair (E, d), where $E \geq 0$ is the allocation to be divided and $d \in \mathbb{R}^N_+$ is the vector of claims such that $\sum_{i\in N} d_i \geq E$. In this paper, we use a bankruptcy rule, namely the proportional rule ($PROP$). The rule $PROP$ is defined by $PROP_i(E, d) = \frac{d_i}{\sum_{i\in N} d_i} E$ for each bankruptcy problem (E, d) and all $i \in N$.

3. **Elliptic Curves.** Cryptography is the most important tool to enhance security of cloud computing, which is possible to make by using symmetric key or public key algorithms. Here, we suggest a novel public key scheme by incorporating the more common Weierstrass curve and the alternate models of elliptic curves. This scheme essentially utilizes an ephemeral-static Elliptic Curve Diffie-Hellman key exchange algorithm. The security of the proposed scheme, which also fulfills the property of semantic security, depends on the difficulty of solving Elliptic Curve Discrete Logarithm Problem (ECDLP) and Elliptic Curve Diffie-Hellman Problem (ECDHP).

3.1. **Introduction to elliptic curves over finite fields.** Let $\mathbb{F}_q$ be a finite field with $q = p^n$. Then the algebraic closure of $\mathbb{F}_q$ is given by $\overline{\mathbb{F}_q} = \bigcup_{i\geq 1} \mathbb{F}_{q^i}$. An elliptic curve over $\mathbb{F}_q$ with characteristic $p > 3$ is the set of solutions in $\overline{\mathbb{F}_q} \times \overline{\mathbb{F}_q}$ of a Weierstrass curve given by

$$E_W : \; y^2 = x^3 + ax + b, \tag{1}$$

with regard to the coefficients $a, b \in \mathbb{F}_q$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$ in $\mathbb{F}_q$. The solution set of E_W over $\mathbb{F}_q$ defines an additive group, extended by the point at infinity (identity element of E_W) denoted by ∞ [40]. The explicit formula in affine coordinates for the addition of two points in the curve E_W defined over $\mathbb{F}_q$ of characteristic $p > 3$ is given by applying the *chord-and-tangent rule*. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be the points on E_W with $P, Q \neq \infty$ and $Q \neq -P$. Then, we briefly give the addition and doubling formula below:

- **Addition:** If $P \neq Q$, then $P + Q = (x_3, y_3)$, where

$$\begin{cases} x_3 = (\dfrac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2, \\ y_3 = (\dfrac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1. \end{cases}$$

- **Doubling:** If $P = Q$, then $2P = (x_3, y_3)$, where

$$\begin{cases} x_3 = (\dfrac{3x_1^2 + a}{2y_1})^2 - 2x_1, \\ y_3 = (\dfrac{3x_1^2 + a}{2y_1})(x_1 - x_3) - y_1. \end{cases}$$

In an analogous way, Weierstrass form of the curves over $\mathbb{F}_q$ with characteristic $p = 2, 3$ can be simplified by a similar formula as above (see [51, Appendix A]).

It is possible to convert the aforementioned point multiplication formula to the different coordinate systems: projective, Jacobian, mixed, etc. [30]. These coordinate systems do not involve field inversions; thus, employing them supplies efficiency. For instance, by applying the method of homogenization with $x = X/Z$ and $y = Y/Z$ for $Z \neq 0$ relation to (1), we have the subsequent homogeneous equation in projective coordinates:

$$E_{W,h} \ : \ Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{2}$$

where $a, b \in \overline{\mathbb{F}_q}$. The curve $E_{W,h}$ has a unique point with coordinate Z equal to 0, namely $(0 : 1 : 0)$, which has been called previously as the point at infinity ∞. On the other side, for a more efficient computation on elliptic curves we can use the alternate forms of elliptic curves, such as Edwards curves, Jacobi intersections and Jacobi quartics, Hessian curves, Huff curves and their variants. The group structure of these curves has already been surveyed in [8, 11]. They also permit the unified addition formula, meaning that the point addition formula can be employed for the doublings; this allows for a resisting against the side-channel attacks.

3.2. **Proposed scheme.** Now, we propose a novel Elliptic Curve ElGamal based encryption scheme, inspired by the works in [7, 37, 38].

Scheme 1. Let E be any models of elliptic curve in affine coordinates over $\mathbb{F}_q$ with characteristic $p > 3$ and P be an agreed-upon and publicly known point of prime order n on the curve E. Let $\mathcal{A}$ and $\mathcal{B}$ be two parties, which correspond to Alice and Bob, respectively. $\mathcal{B}$ randomly selects a static private key $k_{\mathcal{B}}$ in the interval $[1, n-1]$ and he computes his static public key $Q = k_{\mathcal{B}}P$.

Public Parameters: P, Q.

Private Parameters: $k_{\mathcal{A}}, k_{\mathcal{B}}$.

Encryption: $\mathcal{A}$ encrypts a message $m \in F_q$ as follows:

i) $\mathcal{A}$ randomly selects an ephemeral private key $k_{\mathcal{A}}$ in the interval $[1, n-1]$. Then, she computes her ephemeral public key $k_{\mathcal{A}}P$.
ii) $\mathcal{A}$ computes $k_{\mathcal{A}}k_{\mathcal{B}}P = (x_1, y_1)$ using the static public key $Q = k_{\mathcal{B}}P$ of $\mathcal{B}$.
iii) $\mathcal{A}$ calculates $c = m + (x_1 + y_1) \in F_q$. Then, she sends the ciphertext c along with her ephemeral public key $k_{\mathcal{A}}P$.

Decryption: $\mathcal{B}$ recovers the message $m \in F_q$ as follows:

i) $\mathcal{B}$ computes $k_{\mathcal{A}}k_{\mathcal{B}}P = (x_1, y_1)$, using $\mathcal{A}$'s ephemeral public key $k_{\mathcal{A}}P$.
ii) $\mathcal{B}$ calculates $m = c - (x_1 + y_1) \in F_q$.

3.3. **Computational cost of scheme 1.** The novel scheme does not require any multiplication in $\mathbb{F}_q$, because of the encryption and decryption process. The computational costs of novel scheme just depend on the point multiplication of elliptic curves. In total, we have computations of 3 point multiplication; 2 point multiplication for the encryption part, 1 point multiplication for the decryption part. In Table 1, the detailed computational costs of the point multiplication on alternate forms of elliptic curves are stated; they are more deeply analyzed in [11]. Therefore, the costs of proposed scheme vary depending on the forms of elliptic curves and the coordinate systems. Here, **M**, **S** and **D** enumerate the cost of multiplication, squaring and multiplication by a constant in $\mathbb{F}_q$, respectively.

TABLE 1. Cost of arithmetic on alternate forms of elliptic curves.

Form of elliptic curves	**Coordinates**	**Unified addition**
Weierstrass	Projective	11**M**+5**S**+1**D**
Edwards [23]	Projective	10**M**+1**S**+1**D**
Twisted Edwards [9, 31]	Projective	10**M**+1**S**+2**D**
	Inverted	9**M**+1**S**+2**D**
	Extended	9**M**+2**D**
Jacobi Intersections [14]	Projective	13**M**+2**S**+1**D**
Twisted Jacobi Intersections [27]	Projective	13**M**+2**S**+5**D**
Extended Jacobi Quartics [32]	Jacobian	10**M**+3**S**+1**D**
	Extended Projective	8**M**+3**S**+2**D**
Hessian Curves [34]	Projective	12**M**
Generalized Hessian Curves [26]	Projective	12**M**+1**D**
Twisted Hessian Curves [10]	Projective	11**M**
Huff Curves [35]	Projective	11**M**
Generalized Huff Curves [55]	Projective	11**M**+3**D**
New Generalized Huff Curves [20]	Projective	12**M**+4**D**
Extended Huff Curves [48]	Projective	10**M**

3.4. **Security analysis of scheme 1.** First, we raise the subsequent well-known setting and problems about the elliptic curves.

Definition 3.1. Given $P, Q \in E$, the problem of finding an integer a such that $Q = aP$ is called the Elliptic Curve Discrete Logarithm Problem (ECDLP).

Definition 3.2. Given P, aP and bP, the problem of finding abP is called the Elliptic Curve Diffie-Hellman Problem (ECDHP).

It is evident that the proposed scheme is tractable if one can solve both ECDLP and ECDHP. On the other hand, the security of the scheme depends on identifying the pairwise point $k_{\mathcal{A}}k_{\mathcal{B}}P = (x_1, y_1)$ from $x_1 + y_1 \in \mathbb{F}_q$. In [47], it is proved that there exist $\frac{q-1}{2}$ ways to split $x_1 + y_1 \in \mathbb{F}_q$. However, as far as we survey, there is no methodology known yet to identify the pairwise point $k_{\mathcal{A}}k_{\mathcal{B}}P = (x_1, y_1)$ among them.

Lemma 3.3. *Scheme 1 is* ***semantically secure****.*

Proof. Suppose that $m_1 \in \mathbb{F}_q$ and $m_2 \in \mathbb{F}_q$ are two known messages from the enemy $\mathcal{E}$, and $\mathcal{E}$ sends these two messages to $\mathcal{A}$ for encryption. $\mathcal{A}$ encrypts the message m_1 or m_2 using $k_{\mathcal{A}}k_{\mathcal{B}}P = (x_1, y_1)$ such that $c = m + (x_1 + y_1)$, and she sends the ciphertext c to the enemy $\mathcal{E}$. Hence, by using c, m_1, m_2 and public parameters, $\mathcal{E}$ can receive $c - m_1 = d_1 + (x_1 + y_1)$ (resp. $c - m_2 = d_2 + (x_1 + y_1)$) by substracting m_1 (resp. m_2) from c, where $d_1 = m - m_1$ (resp. $d_2 = m - m_2$). This fact implies that computing d_1 (resp. d_2) is equivalent with identifying the pairwise point $k_{\mathcal{A}}k_{\mathcal{B}}P = (x_1, y_1)$ from $x_1 + y_1$, which is not possible. Consequently, $\mathcal{E}$ is not able to find whether the ciphertext c is the encryption of m_1 or m_2 with a probability non-negligibly larger than $1/2$. □

4. An application: The cooperative interval game model in social networks.

4.1. **Amazon web services.** Amazon Web Services (AWS) are a scable cloud-computing platform constructed for high availability and dependability that provides tools enabling us to run a wide range of applications. In this study, we utilize the subsequently named web services as follows: Amazon Elastic Compute Control (Amazon EC2) is a web service providing a resizable computational capacity within the cloud. It is designed to make web-scale cloud computing easier for developers. Amazon S3 is storage for the Internet and it is constructed to make web-scale computing easier for developers. Amazon Route 53 is a highly available and scable DNS (Domain Name Server) service, which is constructed to give developers a cost effective way to route users for Internet applications. Amazon CloudFront is a web service for content delivery, which delivers content using a global network of edge locations and works seamlessly with Amazon S3, that permanently stores the original versions of files. Amazon RDS is a web service which facilitates it to set up, operate, and scale a relational database in the cloud. Amazon DynamoDB is a high performance non-relational database service, which is easy to set up, operate, and scale. It is created to handle basic problems of database management, performance, scalability, and reliability. It also provides a predictable high performance and a low latency at scale [6].

4.2. **The model.** In our study, it is presumed that we have 3 new social network companies launching social web applications. These websites are three-tier web applications, leveraging open-source content management and publishing soft wares, store and serve large amounts of static media content through content delivery networks, and use relational databases to deliver a personalized user experience to their visitors. These three companies pursue common objectives in terms of work safety. The data of website users are encrypted in a cryptology system; then the companies keep their own user's data in each others' data storage. In this way, the companies aim to demonstrate a reliable network configuration. However, the companies do not have any historical data or experience in launching such an application. This "enterprise" has the potential to bring in a lot of advertising revenue, but they have no idea whether the websites be useful.

To support the websites, each company has got 1 Load Balancer, 2 Web Servers, 2 Application Servers, and 6 High Availability Database Servers. In the two-coalitions, however, the companies use 1 Web Server, 1 Application Server and 4 High Availability Database Servers. In the grand coalition, they use 6 High Availability Database Servers. The type of these servers in all the coalitions are Linux on m4.4xlarge. The properties of Social Network Companies (SNC) and some additional storage for cloud computing services are stated in Table 2.

An illustration of our model's Amazon Cloud Services can be seen in Figure 1.

Here, cost accounting and pricing mechanisms for social network firms are received. The cryptology system as a source locates in the private cloud for safety reasons. The social network companies are placed in a public cloud; herewith, the model runs on a hybrid cloud. The cryptology part of the model refers to Platform as a Service (PaaS) (for details see [38]).

The companies strive to move data from an unencrypted volume to an encrypted volume. They create a snapshot of the unencrypted volume, then they create an unencrypted copy of that snapshot and, finally, restore the encrypted snapshot to

TABLE 2. The parameters of companies.

PARAMETERS	SNC1	SNC2	SNC3	SNC1-SNC2	SNC1-SNC3	SNC2-SNC3	SNC1-SNC2-SNC3
Load Balancer (GB/Month) for EC2	500	500	3000	1000	3500	3500	4000
Web Server (Year/Piece) for EC2	1/2	1/2	1/2	1/4	1/4	1/4	1/6
App Server (Year/Piece) for EC2	1/2	1/2	1/2	1/4	1/4	1/4	1/6
Storage: EBS Volume (Volume/GB) for EC2	6/2500	6/3000	6/8000	12/5500	12/10500	12/11000	18/13500
Storage (TB) for S3	10	100	200	110	210	300	310
Data Transfer Out (GB/Month) for EC2	200	900	6400	1100	6600	7300	7700
Data Transfer In (GB/Month) for EC2	1000	500	10000	1500	11000	10500	11500
Data Transfer Out (GB/Month) for CloudFront	1000	3000	10000	4000	11000	13000	11000
Data Storage (TB) for Dynoma	30	200	350	230	380	550	380
Data Transfer Out (GB/Month) for Dynoma	200	250	1500	450	17000	1750	1700

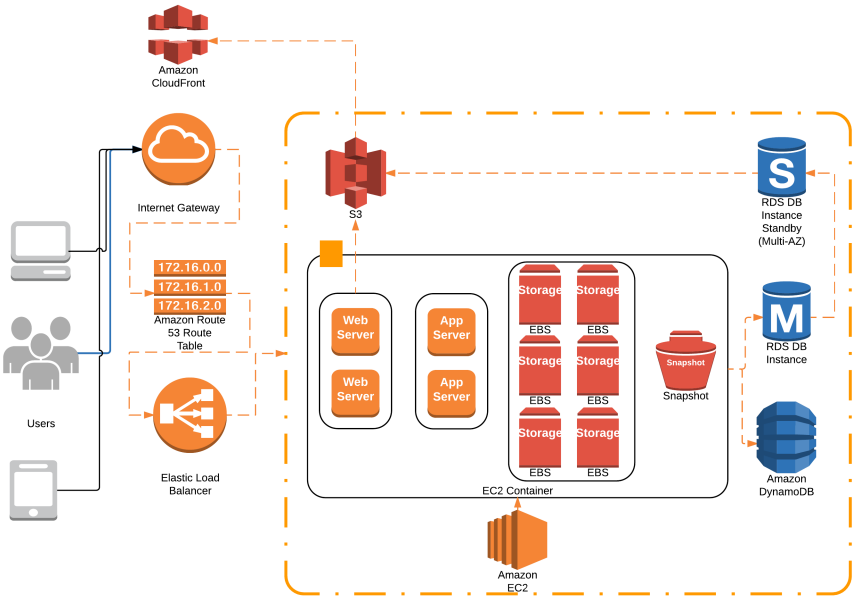

FIGURE 1. The Amazon Cloud Service properties of one social network company.

a new volume (the other companies' data store), which will also be encrypted. The model with cryptology system works for this target and creates cryptographic costs to the companies.

There is uncertainty about the realization of a snapshot creation, about the process in one day, and the cryptographic cost is taken as a degenerate internal. We assume that there exists a standard cost in cryptography (see Section 3). In order to work on the ambiguity levels of 0% and 100%, respectively, we use the cooperative game under interval uncertainty. The total costs of Amazon Web Services for each company and each coalitions can be found in Table 3.

TABLE 3. The total costs.

Amazon Web Services	Total Cost of Company ($) ([0%, 100%])
SNC1	[13063.02, 35506.80]
SNC2	[64401.07, 91333.57]
SNC3	[116776.67, 188596.67]
SNC1-SNC2	[41587.70, 81986.54]
SNC1-SNC3	[141710.26, 330237.82]
SNC2-SNC3	[193574.13, 391079.13]
SNC1-SNC2-SNC3	[168389.68, 531978.52]

In the model, $\psi = [\underline{\psi}, \underline{\psi}]$, being the cost of the required proposed encryption algorithm (Scheme 1) is added to the costs constructed from the social network companies and the cryptology system. Then, the following costs are respectively obtained: $[13063.02 + \underline{\psi}, 35506.80 + \underline{\psi}]$, $[64401.07 + \underline{\psi}, 91333.57 + \underline{\psi}]$, $[116776.67 + \underline{\psi}, 188596.67 + \underline{\psi}]$. Hence, the total costs are calculated from storing the encrypted information of other social network companies' data stores. Figure 2 illustrates the model with closer details.

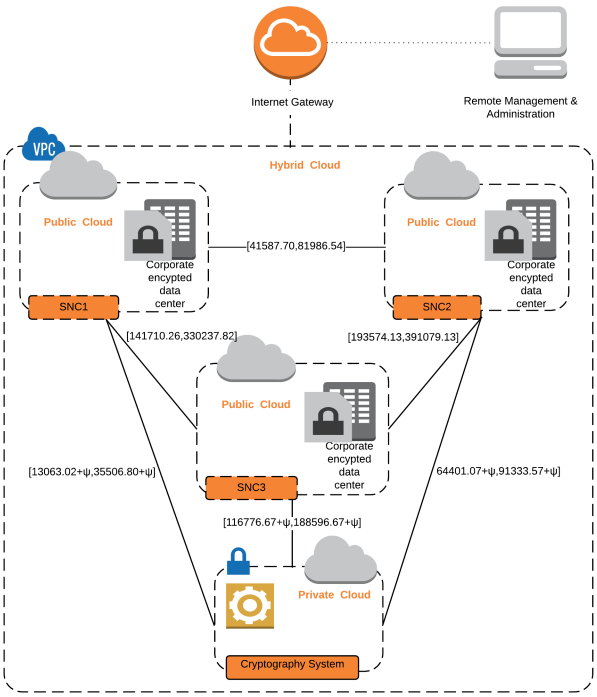

FIGURE 2. The crypto-computing model of the study.

4.3. **The interval solutions.** In our model, social network cloud services are constructed in a cooperative manner. In the sequel, the costs are allocated by using

the interval Bird rule and the interval Shapley value. We note that $\psi = [\underline{\psi}, \overline{\psi}]$ is our encryption cost. First, we use the Bird rule (see Figure 2). Then, the optimal solution is $\left[196360.98 + \underline{\psi}, 447731.16 + \overline{\psi}\right]$. This yields us the *Bird allocation* $\beta^R(\Gamma)$ as follows:

$$\begin{aligned}\beta^R(\Gamma) &= \big([13063.02 + \underline{\psi}, 35506.80 + \overline{\psi}], [41587.70, 81986.54],\\ &\quad [141710.26, 330237.82]\big).\end{aligned}$$

Table 4 illustrates the interval costs of the coalitions.

TABLE 4. The interval costs of the coalitions.

$c(\{\emptyset\}) = [0, 0]$
$c(\{1\}) = \left[13063.02 + \underline{\psi}, 35506.80 + \overline{\psi}\right]$
$c(\{2\}) = \left[64401.07 + \underline{\psi}, 91333.57 + \overline{\psi}\right]$
$c(\{3\}) = \left[116776.67 + \underline{\psi}, 188596.67 + \overline{\psi}\right]$
$c(\{1,2\}) = \left[54650.72 + \underline{\psi}, 117493.34 + \overline{\psi}\right]$
$c(\{1,3\}) = \left[154773.28 + \underline{\psi}, 365744.62 + \overline{\psi}\right]$
$c(\{2,3\}) = \left[257975.2 + \underline{\psi}, 482412.7 + \overline{\psi}\right]$
$c(\{1,2,3\}) = \left[196360.98 + \underline{\psi}, 447731.16 + \overline{\psi}\right]$

Second, we calculate the interval Shapley value $\Phi(c)$ of our game as follows:

$$\begin{aligned}\Phi(c) &= \big([-11476.02 + \underline{\psi}/3, 34159.71 + \overline{\psi}/3],\\ &\quad [65793.96 + \underline{\psi}/3, 120407.13 + \overline{\psi}/3],\\ &\quad [142043.04 + \underline{\psi}/3, 293164.32 + \overline{\psi}/3]\big).\end{aligned}$$

4.4. **The PROP rule.** In this section, we suggest a one-point solution by the help of our interval solutions. Here, we apply the proportional rule (PROP) to get a one-point solution from an interval solution (for details see [17]).

First, we employ the interval Bird rule and assume that the realizations of $c(N)$ are $R_1 = 200000 + \underline{\psi}, R_2 = 250000 + \underline{\psi}$, $R_3 = 450000 + \overline{\psi}$.

Now, we calculate the individual crisp allocations. Then, we distribute the amount $E_i, i = 1, 2, 3$, among three social network companies as follows:

$$\begin{aligned}E_1 &= R_1 - \underline{c}(N) = 3639.02,\\ E_2 &= R_2 - \underline{c}(N) = 53639.02,\\ E_3 &= R_3 - \underline{c}(N) = 253639.02,\end{aligned}$$

The claims $d_i, i = 1, 2, 3$, of each company on the realizations R_1, R_2, R_3 are as follows:

$$\begin{aligned}d_1 &= \overline{J}_1 - \underline{J}_1 = 22443.78,\\ d_2 &= \overline{J}_2 - \underline{J}_2 = 40398.84,\\ d_3 &= \overline{J}_3 - \underline{J}_3 = 188527.56.\end{aligned}$$

We note that the total claim is 251370.18. Table 5 illustrates the one-point PROP solution by using interval Bird rule.

Second, we apply the interval Shapley rule.

TABLE 5. The one-point solutions by using PROP for the interval Bird rule.

f	d
$PROP(E_1, d)$	$(324.91, 584.83, 2729.26)$
$PROP(E_2, d)$	$(4789.20, 8620.57, 40229.25)$
$PROP(E_3, d)$	$(22646.36, 40763.47, 190229.19)$

The claims $d_i, i = 1, 2, 3$, of each company on the realizations R_1, R_2, R_3 are as follows:

$$\begin{aligned} d_1 = &\quad \overline{J}_1 - \underline{J}_1 = \quad 45635.73, \\ d_2 = &\quad \overline{J}_2 - \underline{J}_2 = \quad 54613.17, \\ d_3 = &\quad \overline{J}_3 - \underline{J}_3 = \quad 151121.28. \end{aligned}$$

We note that the total claim is 251370.18. Table 6 illustrates the one-point PROP solution by using interval Shapley rule.

TABLE 6. The one-point solutions by using PROP for the interval Shapley rule.

f	d
$PROP(E_1, d)$	$(660.66, 790.62, 2187.74)$
$PROP(E_2, d)$	$(9738.05, 11653.72, 32247.25)$
$PROP(E_3, d)$	$(46047.64, 55106.10, 152485.28)$

5. **Conclusion.** Recently, Crypto Cloud Computing has become an interesting research area with many technical, security, commercial and financial aspects, goals and consequences. Cloud computing comes along with its share of challenges, in terms of security, data privacy, compliance, availability, lack of standards, etc. These challenges are highlighted more in regulated and security-sensitive environments, such as Social Networks. Considering the cooperative functionality of Crypto Cloud Computing, the use of game theory in that area has been understood to become very beneficial [1, 19, 38].

Uncertainty is present in almost every real-world situation, it is influencing and questioning our decisions. What in the past is regarded as a matter left alone to the soft human and social sciences, now enters core areas of hard research, computation and calibration. This has been transforming the view on uncertainty, supported by approaches such as uncertainty quantization, grey numbers, robust counterparts of optimization and of stochastic optimal control, e.g. related to stochastic hybrid systems with jumps [36, 41, 49, 53].

In this study, we construct a model by using cooperative game theory under uncertainty, which associates to Crypto Cloud Computing. In the sequel, we propose a novel encryption algorithm by using elliptic curves over finite fields having the property of semantic security. Hence, we retrieve data from the database of Amazon Web Service. The most interesting and important property of our work is

combining the cryptography and cooperative game theory in social networks used in cloud-computing applications. By implementing the cryptographic solution to the cooperative interval games, we both must be behind from cooperative game and cryptography sides. Before closing, we note that our study deals with cooperative interval games without any probability included. However, in future research and application, our model and related solution concepts can be applied to the different forms such as stochastic, fuzzy or grey uncertainty [44, 49, 53].

Acknowledgments. We thank the anonymous referees for their detailed and very helpful comments. Furthermore, we express our gratitude to Editor-in-Chief, Professor Kok Lay Teo, and Associate Editor of the paper, Professor Stefan Wolfgang Pickl.

REFERENCES

[1] S. P. Ahuja and B. Moore, A Survey of Cloud Computing and Social Networks, *Network and Communication Technologies*, **2** (2013), 11–16.
[2] S. Z. Alparslan Gök, R. Branzei and S. Tijs, The interval Shapley value: an axiomatization, *Central European Journal of Operations Research*, **18** (2010), 131–140.
[3] S. Z. Alparslan Gök, R. Branzei and S. Tijs, Convex interval games, *Journal of Applied Mathematics and Decision Sciences*, *2009* (2009), Article ID 342089, 14 pages.
[4] S. Z. Alparslan Gök, O. Palancıand M. O. Olgun, Cooperative interval games: Mountain situations with interval data, *Journal of Computational and Applied Mathematics*, **259** (2014), 622–632.
[5] S. Z. Alparslan Gök and G.-W. Weber, On dominance core and stable sets for cooperative ellipsoidal games, *Optimization*, **62** (2013), 1297–1308.
[6] Amazon Web Services, Available from: `http://calculator.s3.amazonaws.com/index.html`.
[7] M. Ashraf and B. B. Kırlar, Message transmission for GH- public key cryptosystem, *Journal of Computational and Applied Mathematics*, **259** (2014), 578–585.
[8] M. Ashraf and B. B. Kırlar, On the Alternate Models of Elliptic Curves, *International Journal of Information Security Science*, **1** (2012), 49–66.
[9] D. Bernstein, P. Birkner, M. Joye, T. Lange and C. Peters, Twisted Edwards curves, *Progress in Cryptology - Africacrypt 2008, Lecture Notes in Computer Science*, **5023** (2008), Springer, 389–405.
[10] D. Bernstein, C. Chuengsatiansup, D. Kohel and T. Lange, Twisted Hessian curves, *Progress in CryptologyLATINCRYPT 2015,* 269–294, Lecture Notes in Comput. Sci., 9230, Springer, Cham, 2015. Available from `https://eprint.iacr.org/2015/781.pdf`.
[11] D. Bernstein and T. Lange, Explicit Formulas Database, Available from `http://www.hyperelliptic.org/EFD`.
[12] D. Bernstein and T. Lange, Faster addition and doubling on elliptic curves, *Progress in Cryptology - Asiacrypt 2007, Lecture Notes in Computer Science*, **4833** (2007), Springer, 29–50.
[13] D. Bernstein, T. Lange and R. R. Farashahi, Binary Edwards Curves, *Cryptographic Hardware and Embedded Systems - CHES 2008, Lecture Notes in Computer Science*, **5154** (2008), Springer, 244–265.
[14] O. Billet and M. Joye, The Jacobi model of an elliptic curve and side-channel analysis, *AAECC 2003, Lecture Notes in Computer Science,* **2643** (2003), Springer-Verlag, 34–42.
[15] C. G. Bird, On cost allocation for a spanning tree: A game theoretic approach, *Networks*, **6** (1976), 335–350.
[16] P. Borm, H. Hamers and R. Hendrickx, Operations research games: A survey, *TOP*, **9** (2001), 139–216.
[17] R. Branzei, S. Tijs and S. Z. Alparslan Gök, How to handle interval solutions for cooperative interval games, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, **18** (2010), 123–132.
[18] R. Branzei, S. Z. Alparslan Gök and O. Branzei, Cooperative games under interval uncertainty: on the convexity of the interval undominated cores, *Central European Journal of Operations Research*, **19** (2011), 523–532.

[19] K. Chard, S. Caton, O. Rana and K. Bubendorfer, Social cloud: Cloud computing in social networks, IEEE 3rd International Conference on Cloud Computing, (2010), 99–106.
[20] A. A. Ciss and D. Sow, On a New Generalization of Huff Curves, 2011. Available from http://eprint.iacr.org/2011/580.pdf.
[21] A. Claus and D. J. Kleitman, Cost allocation for a spanning tree, *Networks*, **3** (1973), 289–304.
[22] J. Devigne and M. Joye, Binary Huff Curves, *Topics in Cryptology - CT-RSA 2011, Lecture Notes in Computer Science,* **6558** (2011), Springer, 340–355.
[23] H. Edwards, A normal form for elliptic curves, *Bulletin of the American Mathematical Society*, **44** (2007), 393–422.
[24] J. R. Evans and E. Minieka, *Optimization Algorithms for Networks and Graphs*, CRC Press, 1992.
[25] K. A. Falahi, Y. Atif and S. Elnaffar, Social networks: Challenges and new opportunities, In *Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing,* (2010), 804–808.
[26] R. R. Farashahi and M. Joye, Efficient Arithmetic on Hessian Curves, *Public Key Cryptography - PKC 2010, Lecture Notes in Computer Science*, **6056** (2010), Springer, 243–260.
[27] R. Feng, M. Nie and H. Wu, Twisted jacobi intersections curves, *Theory and Applications of Models of Computation*, 2010, 199–210, Available from http://eprint.iacr.org/2009/597.pdf.
[28] D. Granot, Cooperative games in stochastic characteristic function form, *Management Science*, **23** (1977), 621–630.
[29] T. S. Gustavsen and K. Ranestad, A simple point counting algorithm for hessian elliptic curves in characteristic three, *Appl. Algebra Eng. Commun. Comput.*, **17** (2006), 141–150.
[30] D. Hankerson, A. Menezes and S. Vanstone, *Guide to Elliptic Curve Cryptography*, Springer, 2004.
[31] H. Hisil, K. Koon-Ho Wong, G. Carter and E. Dawson, Twisted Edwards Curves Revisited, *Advances in Cryptology - Asiacrypt 2008, Lecture Notes in Computer Science*, **5350** (2008), Springer-Verlag, 326–343.
[32] H. Hisil, K. Koon-Ho Wong, G. Carter and E. Dawson, Jacobi quartic curves revisited, *ACISP*, 2009, 452–468.
[33] G. Huff, Diophantine problems in geometry and elliptic ternary forms, *Duke Math. J.*, **15** (1948), 443–453.
[34] M. Joye and J. Quisquater, Hessian elliptic curves and sidechannel attacks, *Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science*, **2162** (2001), Springer, 402–410.
[35] M. Joye, M. Tibbouchi and D. Vergnaud, Huff's Model for Elliptic Curves, Algorithmic Number Theory - ANTS-IX, Lecture Notes in Computer Science, **6197** (2010), Springer, 234–250.
[36] E. Kilic, A. Karimov and G.-W. Weber, Applications of stochastic hybrid systems in portfolio optimization, In: Thomaidis N, DashGHJr, editors. Recent Advances in Computational Finance. (NY): Nova Science.
[37] B. B. Kırlar and M. Çil, On the k-th order LFSR sequence with public key cryptosystems, *Mathematica Slovaca*, **67** (2017), 601–610.
[38] B. B. Kırlar, S. Ergün, S. Z. Alparslan Gök and G.-W. Weber, A game-theoretical and cryptographical approach to crypto-cloud computing and its economical and financial aspects, *Annals of Operations Research*, **260** (2018), 217–231.
[39] N. Koblitz, Elliptic curve cryptosystems, *Mathematics of Computation*, **48** (1987), 203–209.
[40] N. Koblitz, A. Menezes and S. Vanstone, The State of Elliptic Curve Cryptography, *Designs, Codes and Cryptography*, **19** (2000), 173–193.
[41] E. Kropat, G.-W. Weber and J.-J. Rückmann. Regression analysis for clusters in gene environment networks based on ellipsoidal calculus and optimization. *Dyn. Cont. Dis. Impulsive Syst. Ser. B.*, **17** (2010), 639–657.
[42] P. Liardet and N. Smart, Preventing SPA/DPA in ECC systems using the Jacobi form, *Cryptographic Hardware and Embedded Systems - CHES 2001, Lecture Notes in Computer Science*, **2162** (2001), Springer-Verlag, 391–401.
[43] P. Maillé, P. Reichl and B. Tuffin, Of threats and costs: A game-theoretic approach to security risk management, In: *Performance Models and Risk Management in Communications Systems*, **46** (2011), Springer, New York, 33–53.

[44] M. Mares, *Fuzzy Cooperative Games: Cooperation with Vague Expectations*, Physica Verlag, Heidelberg, 2001.
[45] V. Miller, Use of elliptic curves in cryptography, *Advances in Cryptology – CRYPTO –85, Lecture Notes in Computer Science,* **218** (1986), 417–426.
[46] S. Moretti, S. Z. Alparslan Gök, R. Branzei and S. Tijs, Connection situations under uncertainty and cost monotonic solutions, *Computers & Operations Research*, **38** (2011), 1638–1645.
[47] A. Muratovic-Ribic and Q. Wang, Partitions and Compositions over Finite Fields, *The Electronic Journal of Combinatorics*, **20** (2013), Paper 34, 14 pp.
[48] N. G. Orhon and H. Hisil, Speeding up Huff Form of Elliptic Curves, *Designs, Codes and Cryptography*, **86** (2018), 2807–2823.
[49] O. Palancı, S. Z. Alparslan Gök, S. Ergün and G.-W. Weber, Cooperative grey games and the grey Shapley value, *Optimization*, **64** (2015), 1657–1668.
[50] L. S. Shapley, A value for n-person games, *Annals of Mathematics Studies*, **28** (1953), 307–317.
[51] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, Berlin, 1986.
[52] N. Smart and E. J. Westwood, Point multiplication on ordinary elliptic curves over fields of characteristic three, *Appl. Algebra Eng. Commun. Comput.*, **13** (2003), 485–497.
[53] J. Suijs, P. Borm, A. De Waegenaere and S. Tijs, Cooperative games with stochastic payoffs, *European Journal of Operational Research*, **113** (1999), 193–205.
[54] D. B. West, *Introduction to Graph Theory*, Prentice Hall, Inc., Upper Saddle River, NJ, 1996.
[55] H. Wu and R. Feng, Elliptic curves in Huff's model, *Wuhan University Journal of Natural Sciences*, **17** (2012), 473–480. Available from http://eprint.iacr.org/2010/390.pdf.

Received June 2018; 1st revision October 2018; 2nd revision December 2018.

E-mail address: serapbakioglu@isparta.edu.tr
E-mail address: bariskirlar@sdu.edu.tr, barisbkirlar@gmail.com
E-mail address: zeynepalparslan@yahoo.com
E-mail address: gerhard.weber@put.poznan.pl