KEY AGREEMENT PROTOCOL FOR DISTRIBUTED SECURE MULTICAST FOR eASSESSMENT

Mariana Durcheva and Malinka Ivanova

Technical University of Sofia
e-mails: m_durcheva@tu-sofia.bg, m_ivanova@tu-sofia.bg
Bulgaria

Abstract: eAssessment is typical for online and distance learning, but nowadays it is also applicable in institutions with blended-learning delivery mode, because of advantages that proposes to teachers and learners: performance of online examination in time suitable for learners and from any geolocation, immediate feedback and exam results. In several learning scenarios, the eAssessment could occur in groups where the multicast communication from type one-to-many or man-to-many could be performed. In this case, the arising problem concerns security in collaborative and synchronous environment. It is important to protect all participants from false messaging and illegal behavior. One solution of this problem is implementation of multicast security which main benefits are related to: high scalable, fast re-key operation, decreased network load. The aim of the paper is to present a key exchange protocol for distributed multicast security. The advantage of the protocol is that it offers more security because it relies on the problem for two sided action of two dual semifields which can be reduced to a two-sided linear equation. Such equations have not yet been considered and a general solution for them has so far not been found in polynomial time.

Key words: eAssessment, security, multicast, protocol for distributed key agreement, idempotent semirings.

1. INTRODUCTION

eAssessment is defined as a method or a set of methods for assessment of students learning performance and/or learning outcomes as well as for evaluation of achieved competences and/or skills through usage of a wide variety of technologies [1], [2] and [3]. eAssessment takes different forms and types and it depends on the educational scenario and context. In some scenarios, the eAssessment occurs in environments with tools for online synchronous communication among students and educators. Students could perform assessment activities individually, in small groups or collaboratively. According to von Davier and Halpin there are three types of teams where the learners' collaborative interactions depend on the actions of their collaborators: ensemble, group and synchronized individuals [4]. Collaborative assessment gives possibility to all members of a learning community to assess tasks of a learner sharing their constructive criticism [5]. In [4] is given the difference among ensemble, group and synchronized individuals. In an ensemble the team tasks could be accomplished only through collaborative work of all team members, they

cannot work in isolation. In a group every member performs a task individually contributing to the team progress. Synchronized individuals also form a team where every member works in isolation, but their tasks are synchronized in time. Other form for collaboration is performance of peer-to-peer assessment activities where students review the generated results of their classmates [6]. An innovative model for assessment is proposed by Yuste et al. who combine videoconferencing with assessment tasks [7]. The power of the method is in the continuous assessment of tasks, projects and interviews applicable at online training. Anyway, it is tested for formative assessment too and shows positive results. Also, Chen et al. talk about synchronous assessment and its potential usage for online courses improvement [8]. The authors propose four types of synchronous eAssessment: synchronous quiz, synchronous written test, synchronous oral examination and synchronous assessment of practical tasks. Thomas et al. share the student experience at synchronous examination enrolled in a distance course [9]. They report positive students' opinion concerning electronic examination from home. As it can be seen, the eAssessment is typical for online and distance education, but it is applicable also in blended-learning educational form, where combination of online and offline modes of examination are possible [10], [11]. Practices show that eAssessment process occurs in distributed eLearning environments in many of cases for training and educational institutions where learners and teachers perform a wide range of assessment activities accessible via Internet. Figure 1 summarizes several cases of synchronous and/or collaborative eAssessment:

- Learners perform assessment activities in collaboration (teams are created inthe form of ensemble, group or working as synchronized learners) and the teacher assesses the result/product.
- The learner is assessed by the teacher through synchronous assessment activity – for example oral communication through usage of audio/video conferencing.
- Peer-to-peer assessment in collaborative environment, where one peer assesses other peer.

Because all assessment activities are performed in the web, an emerged problem is related to the secure transfer and storage of private and operable data during the eAssessment process.

This paper presents the current situation in the area of security during online examination, showing the existing practices. Then, we propose a new solution for security, based on protocol for distributed key agreement over idempotent semirings. Multicasting is defined as the ability to transmit a single stream to multiple subscribers at the same time [12]. The multicast security protocols are focused on the problem of key management. The goal of the key management is to distribute the group key securely to the group members who can then use it to encrypt or decrypt the multicast data. They deal with the number of key messages exchanged with increasing group size.

The aim of the paper is to present a key exchange protocol for distributed multicast security. For this purpose, firstly, the main assessment activities typical for an eAsessment process are discussed and several important security issues are pointed out. Then, after summarization and analysis of existing solutions and best practices concerning secure eAssessment process, a model of a cryptosystem based on multicast security protocol is proposed.

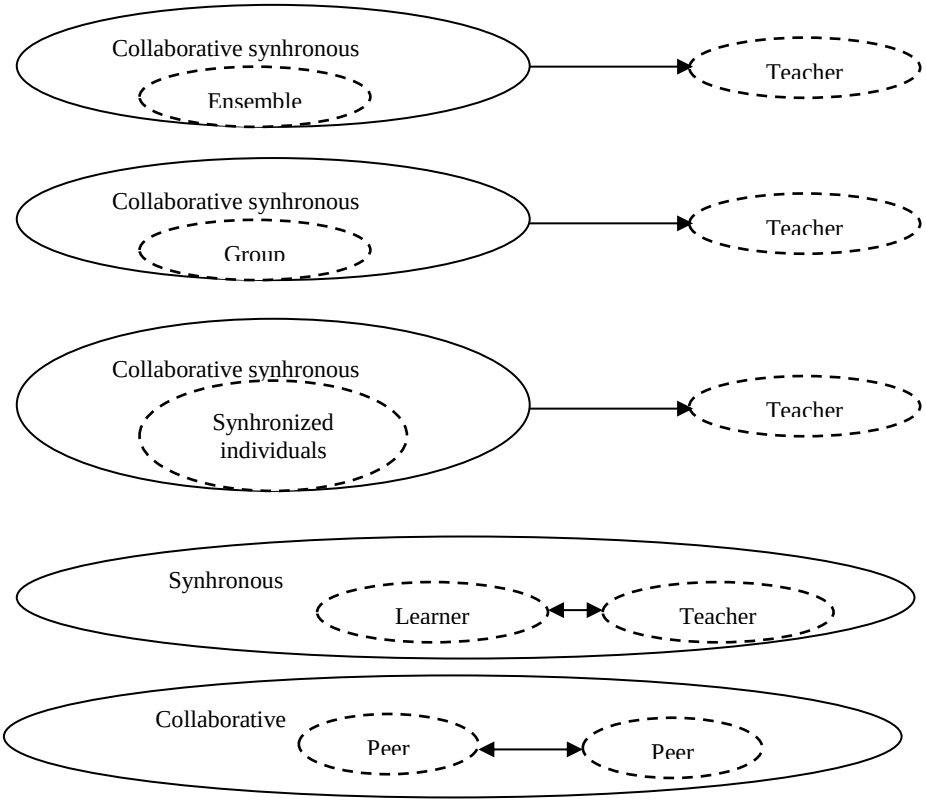

Fig. 1. Synchronous and/or collaborative eAssessment

2. CURENT SITUATION IN THE AREA OF SECURITY DURING ONLINE EXAMINATION

The literature review shows that a multicast communication takes place in applications for videoconferencing, audio/video streaming, stock market quotes, distributed games, training systems. Also, the multicasting is applicable in the area of online examination and researchers are looking for techniques and algorithms to secure interactions. The difficulties of security come from the fact that the sender could be even somebody outside the group, and also, the received data cannot be customized. The multicasting security issues in online examination are related to: (1) the correct authentication – correct identification of the group members (teachers and learners), (2) ensuring the access control to the group – who can be a member from this group and who can send data to the group members, (3) the correct key management for ensuring the data integrity and confidentiality and (4) the fingerprinting – customization and individualization of the data transmitted to the receivers.

The subject of security of multicasting in the context of eAsessment is immature and just a few publications were in the scope of this research.

Zhang et al. in [13] present a layered degree-constrained overlay multicast (LDCOM) protocol that is applied to resolve the conflicts in the case of dynamic interaction and live

streaming as well as to guarantee the maximum delay of the shared interaction. The protocol is utilized at realization of a live teaching system ensuring synchronous collaborative interactions. The performed experiment shows that the created prototype with LDCOM method has the possibility to support one-way live streaming at large scale and two-way interaction between participants and tutor and also to guarantee the delay.

Granda et al. propose a networking technique for multimedia data delivery in real time through usage of IP multicast (see [14]). This technique is utilized in development of multimedia applications for e-learning where synchronous communication has to connect employees from different multinational corporations located in different geographical places. The results confirm the efficiency of this technique in comparison to unicast data delivery.

Kiah and Martin present a host protocol for safe movement of group members from one area to other as well as their return to visited places in wireless mobile environment [15]. The protocol is applicable in the case of group communication at solutions of multimedia conferencing and virtual classroom e.g. in applications with multicast functionality. For efficient management of members' movement, the protocol includes a mechanism "Mob-List" where all movements are registered. The security problems in the context of multicast application in eAssessment are summarized in three groups and they are related to:

- Multicast group formation- Who has possibility to send data to group members? How the sender to be identified? How a new member can join the group? How a member will leave the group? How the group member individualization/customization could be performed?
- Communication in the group – the communication scenarios are: one sender to many receivers and many senders to many receivers;
- Key management – it includes individual key formation, group key generation and cases for re-keying.

3. IDEMPOTENT SEMIRINGS

3.1. Preliminaries

Semiring in [16] and [17] is called a nonempty set S with two binary operations: addition (+) and multiplication (·). These operations have the following properties:

1. $(S,+)$ is a commutative semigroup i.e. $x+y=y+x$ and $x+(y+z)=(x+y)+z$ for all $x,y,z\in S$
2. $(S,\cdot)$ is a semigroup i.e. $x\cdot(y\cdot z)=(x\cdot y)\cdot z$ for all $x,y,z\in S$
3. two distributive laws hold: $x\cdot(y+z)=x\cdot y+x\cdot z$ and $(x+y)\cdot z=x\cdot z+y\cdot z$ for all $x,y,z\in S$.

Let $S=(S,+,\cdot)$ be a semiring. Then:

- If a neutral element 0 for a semigroup $(S,+)$ exists, i.e. $x+0=0+x=x$ for all $x\in S$ and $x\cdot 0=0\cdot x=x$ for all $x\in S$, the neutral element is called *zero*.
- If a neutral element ε for a semigroup $(S,\cdot)$ exists, i.e. $x\cdot 0=0\cdot x=x$ for all $x\in R$ and $x\cdot\varepsilon=\varepsilon\cdot x=x$ for all $x\in S$, the neutral element is called *one*.

We will note that some authors (see [18]) define a semiring as a structure with zero and one.

The semiring $(S,+,\cdot)$ is called *commutative* if the semigroup $(S,\cdot)$ is commutative.

An element a of a semiring $(S,+,\cdot)$ is called an *additively* (*multiplicatively*) *absorbing* if the following equality $a+x=a$ ($a\cdot x=x\cdot a=a$) holds for all $x\in S$. An element which is both additively and multiplicatively absorbing is called *infinity* and is denoted by ∞.

An element a of a semiring $(S,+,\cdot)$ is called an *additively idempotent* if $a+a=a$. If every element of a semiring is an additively idempotent then the semiring is called an *additively idempotent semiring.* An element a of a semiring $(S,+,\cdot)$ is called a *multiplicatively idempotent* if $a\cdot a=a$. If a semiring S is an additively idempotent, then its multiplicatively idempotent elements are called *idempotent elements*, or *idempotents*. A semiring $(S,+,\cdot)$ is called an *idempotent* if it is an additively idempotent**.**

If a semiring $(S,+,\cdot)$ has a zero element 0, let us denote $S^*=S\setminus\{0\}$, and if S does not have zero, we denote $S^*=S$. Then if $(S^*,\cdot)$ is a group, the semiring S is called a *semifield*. A semiring S with one is called a *semifield* if each nonzero element of it has an opposite element with respect to multiplication.

A semiring $S_{\max,\min}=\langle R\cup\{-\infty,+\infty\},\max,\min\rangle,$ is an idempotent semiring which is not a semifield. For this semiring $0=-\infty,\varepsilon=+\infty$. The opposite element with respect to the operation *min* does not exist. The maximal element of this semiring is $+\infty$.

In this paper we are interested in four idempotent semifields, namely:

$$S_{\max,+}=\langle R\cup\{-\infty\},\max,+\rangle,\qquad S_{\min,+}=\langle R\cup\{+\infty\},\min,+\rangle,$$

$$S_{\max,\times}=\langle R_+\cup\{0\},\max,\times\rangle,\qquad S_{\min,\times}=\langle R_+\cup\{+\infty\},\min,\times\rangle,$$

where *R* is the field of real numbers and $R_+=\{x\in R\,|\,x>0\}$, "+" is usual addition, "$\times$" is usual multiplication. Let us point out that for the semiring $S_{\max,+}$ the additional operation is maximum and the multiplicational is "+", for the semiring $S_{\min,+}$ the additional operation is minimum and the multiplicational is "+", for the semiring $S_{\max,\times}$ the additional operation is maximum and the multiplicational is "$\times$", for the semiring $S_{\min,\times}$ the additional operation is minimum and the multiplicational is "$\times$".

3.2 Dual idempotent semirings

Let $G=\langle G,\le,\otimes\rangle$ be a group which has a lattice structure. We join two new elements $\perp$ and T and obtain $\overline{G}=G\cup\{\perp,\mathrm{T}\}$. Thus, we extend the ordinance in the group as follows: $\perp\le a\le\mathrm{T}$ for all $a\in\overline{G}$. The operation in the group can be also extended, namely:

$$a \otimes_{\bullet} b = \begin{cases} \perp & \text{if} \quad a,b \in G \cup \{\perp, \mathrm{T}\} \quad or \quad a = \perp \quad or \quad b = \mathrm{T}, \\ \mathrm{T} & if \quad a,b \in G \cup \{\mathrm{T}\} \quad or \quad a = \mathrm{T} \quad or \quad b = \mathrm{T}, \\ a \otimes b & if \quad a,b \in G, \end{cases}$$

$$a \otimes^{\bullet} b = \begin{cases} \mathrm{T} & \text{if} \quad a,b \in G \cup \{\perp, \mathrm{T}\} \quad or \quad a = \mathrm{T} \quad or \quad b = \mathrm{T}, \\ \perp & if \quad a,b \in G \cup \{\mathrm{T}\} \quad or \quad a = \perp \quad or \quad b = \perp, \\ a \otimes b & if \quad a,b \in G. \end{cases}$$

The structure $\overline{G} = \langle G, \leq, \otimes_{\bullet}, \otimes^{\bullet} \rangle$ is a canonical extending of the group $G = \langle G, \leq, \otimes \rangle$. The operations $\otimes_{\bullet}$ and $\otimes^{\bullet}$ are associative and commutative over $\overline{G}$. Following this approach to the semiring $S = \langle S, \oplus, \otimes, 0, \varepsilon \rangle$, we first obtain the semiring $\overline{S} = \langle \overline{S}, \oplus_{\bullet}, \otimes_{\bullet}, 0, \varepsilon \rangle$, where the set $\overline{S} = S \cup \{\mathrm{T}\}$ and the operation $\otimes_{\bullet}$ is the above defined, S has a lattice structure and is a multiplicative semiring. The operation $\oplus_{\bullet}$ is defined as follows:

$$a \oplus_{\bullet} b = \begin{cases} \mathrm{T} & if \quad a = \mathrm{T} \quad or \quad b = \mathrm{T} \\ a \oplus b & if \quad a,b \in S. \end{cases},$$

Let $\overline{D}$ be an idempotent semifield which is obtained according to the above construction, i.e. $\overline{D} = \langle \overline{D}, \oplus_{\bullet}, \otimes_{\bullet}, 0, \varepsilon \rangle$ with the top element T. It remains to give the opposite element to this top element. Let us set: $0^{-1} = \mathrm{T}, \mathrm{T}^{-1} = 0$. In this way we find two complete dual semifields:

- Complete semilattice under natural order $\langle \overline{D}, \leq \rangle$, i.e. the structure $\overline{D} = \langle \overline{D}, \oplus_{\bullet} = \vee, \otimes_{\bullet}, \perp, \varepsilon \rangle$.
- Complete semilattice under the dual of the natural order $\langle \overline{D}, \leq^{d} \rangle = \langle \overline{D}, \geq \rangle$, i.e. the structure $\overline{D}^{d} = \langle \overline{D}, \oplus^{\bullet} = \wedge, \otimes^{\bullet}, \mathrm{T}, \varepsilon \rangle$.

For these two dual structure, laws, analogous to the De Morgan laws hold.

3.3. Application of idempotent semirings in cryptography

In 2007 Gérard Maze, Chris Monico and Joachim Rosenthal in [19] discussed for the first time a cryptosystem based on semigroups and semirings. The same year 2007, K. Slavin (see [20]) received US patent for his cryptosystem, applying ideas similar to [19]. Atani (see [21] and [22]) published two cryptosystems, using semimodules over factor-semirings. Dwivedi et al. [23] suggested a protocol based on polynomials over noncommutative factor-semirings. D. Grigoriev and V. Shpilrain in [24] firstly suggested to apply an idempotent

semiring in public key cryptography. M. Durcheva considered different applications of idempotent semirings in public key cryptography (see [25], [26] and [27]).

4. THE PROPOSED PROTOCOL

4.1. Dual semirings action

The idea of this action is two dual idempotent semirings to act over a matrix semiring. Let S be a set and let $\overline{D} = \langle S, \oplus_{\bullet}, \otimes_{\bullet}, \perp, \mathrm{T} \rangle$ and $\overline{D}^{d} = \langle S, \oplus^{\bullet}, \otimes^{\bullet}, \perp, \mathrm{T} \rangle$ be two complete dual semifields (here we denote the minimum element by $\perp$ and maximal element by T) and $\overline{S} = \langle S, \oplus, \otimes, \perp, \mathrm{T} \rangle$. We consider matrix semirings, defined over $\overline{S}$, $\overline{D}$ and $\overline{D}^{d}$. Let these be respectively $M^{n\times n}(\overline{S})$, $M^{n\times n}(\overline{D})$ and $M^{n\times n}(\overline{D}^{d})$. Additionally, we consider polynomials of matrices over two dual semifields. Then if $M \in M^{n\times n}(\overline{D})$, $N \in M^{n\times n}(\overline{D}^{d})$, $X \in M^{n\times n}(\overline{S})$,the action is:

$$((p(M), q(N)), X) \mapsto p(M) \circ X \circ q(N).$$

In general case, the protocol consists of the following: two users agree on a public channel about the dual semifields and three matrices $M \in M^{n\times n}(\overline{D})$, $N \in M^{n\times n}(\overline{D}^{d})$, $X \in M^{n\times n}(\overline{S})$.

1. Alice chooses as a secret key two reduced polynomials (for a polynomial in max plus, min plus, max time and min time algebras there are terms which do not contribute to its value, when these terms are removed, a polynomial is called *reduced*) $p(x)$ (over the semifield $\overline{D}$ and $t(x)$ (over the dual semifield $\overline{D}^{d}$). She computes her public key $A = p(M) \otimes_{\bullet} X \otimes^{\bullet} t(N)$ and sends it to Bob.

2. Bob chooses as a secret key two reduced polynomials $q(x)$ (over the semifield $\overline{D}$) and r(x) (over the dual semifield $\overline{D}^{d}$). He computes his public key $B = q(M) \otimes_{\bullet} X \otimes^{\bullet} r(N)$ and sends it to Alice.

3. Alice computes

$$k_A = p(M) \otimes_{\bullet} B \otimes^{\bullet} t(N) = p(M) \otimes_{\bullet} q(M) \otimes_{\bullet} X \otimes^{\bullet} r(N) \otimes^{\bullet} t(N).$$

4. Bob computes

$$k_B = q(M) \otimes_{\bullet} A \otimes^{\bullet} r(N) = q(M) \otimes_{\bullet} p(M) \otimes_{\bullet} X \otimes^{\bullet} t(N) \otimes^{\bullet} r(N).$$

At the end of the protocol, two users obtain a common secret key $k_A = k_B$.

To break this protocol, an eavesdropper must solve the following:

Problem for two sided action of two dual semifields. For given three matrices $M \in M^{n\times n}(\overline{D})$, $N \in M^{n\times n}(\overline{D}^{d})$, $X \in M^{n\times n}(\overline{S})$, and a matrix

$T \in S_1[M] \otimes_{\bullet} X \otimes^{\bullet} S_2[N]$, find two matrices $U_1 \in S_1[M]$ and $U_2 \in S_2[N]$ such that $T = U_1 \otimes_{\bullet} X \otimes^{\bullet} U_2$.

In our case, the matrix T can be the matrix A, i.e. Alice's public key, or the matrix B, i.e. Bob's public key; $S_1[M]$ and $S_2[N]$ are matrix semirings, generated by matrices M and N respectively. This means that to break the proposed protocol, it is enough the eavesdropper to solve the two sided matrix equation $T = U_1 \otimes_{\bullet} X \otimes^{\bullet} U_2$ for the unknown matrices U_1 and U_2, and for known matrices T and X.

Let $\overline{S} = \langle S, \oplus, \otimes, \perp, \mathrm{T} \rangle$ be an idempotent semifield. Each matrix $A \in \overline{S}^{m \times n}$ defines a transformation from a semimodule $\overline{S}^{n}$ to the semimodule $\overline{S}^{m}$. For two matrices $A, B \in \overline{S}^{m \times n}$ and for an unknown vector $x \in \overline{S}^{n}$, an equation $Ax = Bx$ is called *two-sided linear equation*. For the semirings $S_{\max,+} = \langle R \cup \{-\infty\}, \max, + \rangle$ and $S_{\min,+} = \langle R \cup \{+\infty\}, \min, + \rangle$, the question about the complexity of the two-sided linear equation is solved. In [28] is established that it can be reduced in polynomial time to the so called *mean payoff game* problem [29] which is proved to be of the type **NP∩coNP** (see [30]). For some special cases (see, for instance [31], [32]), the solutions of the two-sided linear equation can be found in polynomial time and these cases must be avoided for cryptographic purposes. For the semirings

$$S_{\max,\times} = \langle R_{+} \cup \{0\}, \max, \times \rangle \quad \text{and} \quad S_{\min,\times} = \langle R_{+} \cup \{+\infty\}, \min, \times \rangle,$$

we do not now a solution to a polynomial time has been found. The advantage of the proposed protocol is that, in order to be broken, the eavesdropper must solve the two-sided linear equation for two matrices that are from two different semifields. To solve this equation, the only possible way is an exhaustive search, because a general method for solving it is not known yet. And if the dual semirings, matrices and polynomials are carefully chosen, we believe that this problem cannot be solved in polynomial time.

4.2. Distributed Secure Multicast Protocol

The idea of extension of the Diffie-Hellman key exchange protocol for the multicasting is due to Steiner et al. (see [33]). In this paper authors suggested two protocols, and one of them, called CLIQUES, is used of the same authors in [34] for rekeying in Dynamic Peer Groups. Later, this idea is also used by other authors. For instance, J.-J. Climent et al. in [35] employ noncommutative unitary ring of matrices for building the multicast protocol.

In this paper, we use idempotent semirings for building our multicast protocol. Let the peers are denoted by $P_1, P_2, ..., P_l$. Peers agree on the two dual semifields $\overline{D} = \langle S, \oplus_{\bullet}, \otimes_{\bullet}, \perp, \mathrm{T} \rangle$ and $\overline{D}^{d} = \langle S, \oplus^{\bullet}, \otimes^{\bullet}, \perp, \mathrm{T} \rangle$. Let the matrix semirings, defined over $S, \overline{D}$ and $\overline{D}^{d}$ be respectively $M^{n \times n}(\overline{D})$, $M^{n \times n}(\overline{D}^{d})$, $M^{n \times n}(S)$. Then if

$M \in M^{n\times n}(\overline{D}),\ N \in M^{n\times n}(\overline{D}^d)$, $X \in M^{n\times n}(S)$, and $f(x)$ and $g(x)$ be two polynomials of matrices over the dual semifields, the equality

$$f_i(M) \otimes_{\bullet} f_j(M) \otimes_{\bullet} X \otimes_{\bullet} g_j(N) \otimes_{\bullet} g_i(N) =$$
$$f_j(M) \otimes_{\bullet} f_i(M) \otimes_{\bullet} X \otimes^{\bullet} g_i(N) \otimes^{\bullet} g_j(N) \qquad (1)$$

always hods.

This property helps us to build the following protocol:

At the beginning of the Protocol peers select three matrices $M \in M^{n\times n}(\overline{D}),\ N \in M^{n\times n}(\overline{D}^d)$, $X \in M^{n\times n}(S)$ and these matrices are made public. Every user $P_i, i = 1,2,...,l$ chooses two polynomials $f_i(x)$ with coefficients of $\overline{D}$ and $g_i(x)$ with coefficients of $\overline{D}^d$. The pair of polynomials ($f_i(x), g_i(x)$) is the private key for the user P_i.

1. Peer P_1 computes his public key $K_1 = f_1(M) \otimes_{\bullet} X \otimes^{\bullet} g_1(N)$ and transmits K_1 to the peer P_2 .

2. Peer P_2 computes his public keys $K_{2,1} = f_2(M) \otimes_{\bullet} X \otimes^{\bullet} g_2(N)$ and $K_{2,2} = f_2(M) \otimes_{\bullet} K_1 \otimes^{\bullet} g_2(N)$ and transmits ($K_1, K_{2,1}, K_{2,2}$) to the peer P_3.

3. Peer P_3 computes his public keys $K_{3,1} = f_3(M) \otimes_{\bullet} K_1 \otimes^{\bullet} g_3(N)$,

$K_{3,2} = f_3(M) \otimes_{\bullet} K_{2,1} \otimes^{\bullet} g_3(N)$ and $K_{3,3} = f_3(M) \otimes_{\bullet} K_{2,2} \otimes^{\bullet} g_3(N)$ and transmits ($K_{2,2}, K_{3,1}, K_{3,2}, K_{3,3}$) to the peer P_4 .

...

i. Peer Pi computes his public keys $K_{i,1} = f_i(M) \otimes_{\bullet} K_{i-2,i-2} \otimes^{\bullet} g_i(N)$,

$K_{i,2} = f_i(M) \otimes_{\bullet} K_{i-1,1} \otimes^{\bullet} g_i(N), \ldots, K_{i,i} = f_i(M) \otimes_{\bullet} K_{i-1,i-1} \otimes^{\bullet} g_i(N)$ and transmits ($K_{i-1,i-1}, K_{i,1}, K_{i,2}, ..., K_{i,i-1}, K_{i,i}$) to the peer P_{i+1} .

...

l. The last peer P_l computes public keys $K_{l,1} = f_l(M) \otimes_{\bullet} K_{l-2,l-2} \otimes^{\bullet} g_l(N)$,

$K_{l,2} = f_l(M) \otimes_{\bullet} K_{l-1,1} \otimes^{\bullet} g_l(N), \ldots, K_{l,l} = f_l(M) \otimes_{\bullet} K_{l-1,l-1} \otimes^{\bullet} g_l(N)$ and transmits to the peers $P_1, P_2, ..., P_{l-1}$ the keys ($K_{l,1}, K_{l,2}, ..., K_{l,l-1}$.).

At the end of the protocol, all peers receive a secret key:

$A_i = f_i(M) \otimes_{\bullet} K_{l,l-i} \otimes^{\bullet} g_i(N)$ for $i = 1,2,...,l-1$.

For the last peer P_l, the secret key is $A_l = K_{l,l}$.

Theorem 1. All users (peers) of the proposed protocol (all members of the group) obtain the same secret key $A_1 = A_2 = ... = A_l$.

Proof. The peer P_l computes $A_l = f_l(M) \otimes_{\bullet} K_{l-1,l-1} \otimes^{\bullet} g_l(N) = ... =$

$f_l(M) \otimes_{\bullet} f_{l-i}(M) \otimes_{\bullet} ... \otimes_{\bullet} f_1(M) \otimes_{\bullet} X \otimes^{\bullet} g_1(N) \otimes^{\bullet} ... \otimes^{\bullet} g_{l-1}(N) \otimes^{\bullet} g_l(N).$

The peer P_{l-1} computes $A_{l-1} = f_{l-1}(M) \otimes_{\bullet} K_{l,1} \otimes^{\bullet} g_{l-1}(N) =$

$f_{l-1}(M) \otimes_{\bullet} f_l(M) \otimes_{\bullet} K_{l-2,l-2} \otimes^{\bullet} g_l(N) \otimes^{\bullet} g_{l-1}(N) = \ldots =$

$f_{l-1}(M) \otimes_{\bullet} f_l(M) \otimes_{\bullet} f_{l-2}(M) \otimes_{\bullet} ... \otimes_{\bullet} f_1(M) \otimes_{\bullet} X \otimes^{\bullet} g_1(N) \otimes^{\bullet} ...$

$\otimes^{\bullet} g_{l-2}(N) \otimes^{\bullet} g_l(N) \otimes^{\bullet} g_{l-1}(N), \ldots,$

the peer P_1 computes $A_1 = f_1(M) \otimes_{\bullet} K_{l,l-1} \otimes^{\bullet} g_1(N) = ...$

$f_1(M) \otimes_{\bullet} f_l(M) \otimes_{\bullet} K_{l-2,l-2} \otimes^{\bullet} g_l(N) \otimes^{\bullet} g_1(N) = \ldots =$

$f_1(M) \otimes_{\bullet} f_l(M) \otimes_{\bullet} f_{l-1} \otimes_{\bullet} f_{l-2}(M) \otimes_{\bullet} ... \otimes_{\bullet} f_2(M) \otimes_{\bullet} X \otimes^{\bullet} g_2(N) \otimes^{\bullet} ...$

$\otimes^{\bullet} g_{l-2}(N) \otimes^{\bullet} g_{l-1}(N) \otimes^{\bullet} g_l(N) \otimes^{\bullet} g_1(N).$

According to the equality (1), $A_1 = A_2 = ... = A_l$.

We will point out that the protocol can be extended so that a new peer to join or a peer to leave. In these both cases a rekeying is needed in order to preserve secrecy.

The basis of this protocol is the Protocol 4.1. Therefore, the security of the protocol 4.2 is based on the security of the Problem for two sided action of two dual semifields. As we showed, this problem can be consider as a two-sided linear equation in which two matrices are of two dual idempotent semirings. A general solution in polynomial time of it has so far not been found. That is way we consider that the suggested protocol has a satisfactory level of security.

5. CONCLUSION

In the paper the application of multicast in eAssessment is discussed with different possible scenarios of online examination, extracted from the scientific literature and good practices. Several security problems are identified and the attention is focused on the possible solutions. Then, a distributed multicast protocol based on the properties of the idempotent semifelds is suggested and the correctness of the protocol has been proven. As a future work, this protocol can be extended to meet the requirements for joining and leaving peers, as it is in the real eAssessment process.

REFERENCES

[1] Ridgway, J., S. McCusker, D. Pead. Report 10. *Literature Review of E-assessment*, *http://www.worldclassarena.net/doc/file14.pdf*.

[2] Baleni, Z. Online formative assessment in higher education: Its pros and cons. *The Electronic Journal of e-Learning*, vol. 13, Issue 4, 2015, pp. 228-236.

[3] Gonzáleza, M., F. Jareñoa, R. Lópeza. Impact of Students' Behavior on Continuous Assessment in Higher Education. *https://ruidera.uclm.es.*

[4] von Davier, P., A. Halpin, Collaborative Problem Solving and the Assessment of Cognitive Skills: Psychometric Considerations. 2013, *https://www.ets.org/Media/Research/pdf/RR-13-41.pdf.*

[5] Marcinek, A. Importance of Collaborative Assessment in a 21st Century Classroom. February 16, 2011, *https://www.edutopia.org/blog/collaborative-assessment-digital-classroom-social-media-tools.*

[6] Bader-Natal, A. Combining peer-assistance and peer assessment in a synchronous collaborative learning activity. *https://aribadernatal.com/docs/badernatal/ 2010.pdf.*

[7] Yuste, R., L. Alonso, F. Blázquez. Synchronous Virtual Environments for e-Assessment in Higher Education. *Comunicar 39*, XX 2012, ISSN: 1134-3478, e-ISSN: 1988-3293, pp. 159-167.

[8] Chen, N. et al. Design and Implementation of Synchronous Cyber Assessment and Its Potential Issues. *Proc. of the 17th International Conference on Computers in Education*, 2009, pp. 905-909.

[9] Thomas, P. et al. Remote electronic examination: student experience. *British journal of Educational Technology*, vol. 33, N5, 2002, pp. 537-549.

[10] Shepherd, E. Blended delivery meets e-assessment. in *Khandia, F. (ed.), 11th CAA International Computer Assisted Assessment Conference: Proc. of the Conference*: Lougborough University, pp. 399-402.

[11] State of Victoria (Department of Education and Early Childhood Development), Assessment in online learning environments Digital Learning. *Platforms Research Series Paper* No.3, October 2011.

[12] Banikazemi, M. IP Multicasting: Concepts, Algorithms, and Protocols. *http://www.cse.wustl.edu/~jain/cis788-97/ftp/ip_multicast.pdf*

[13] Zhang, W. et al., An overlay multicast protocol for live streaming and delay-guaranteed interactive media. *Journal of Network and Computer Applications*, 35, 2012, pp. 20-28.

[14] Granda, J. et al. An efficient networking technique for synchronous e-learning platforms in corporate environments. in *Computer Communications*, 33, 2010, pp. 1752-1766.

[15] Mat Kiah, M. L., K. M. Martin. Host Mobility Protocol for Secure Group Communication in Wireless Mobile Environments. *International Journal of Security and its Applications*, vol. 2, No. 1, January, 2008, pp.39-52.

[16] Vandiver, H. S. Note on a simple type of algebra in which cancellation law of addition does not hold. *Bulletin Amer. Math. Soc.* 40, 1934, pp. 914-920.

[17] Hebisch, U., H. J. Weinert. Semirings: algebraic theory and applications in computer science. in *Series in Algebra*, vol. 5, World Scientific Publishing Co. Inc., River Edge, NJ, 1998.

[18] Golan, J. Semirings and Their Applications. *Kluwer*, Dordrecht, 1999.

[19] Maze, G., C. Monico, J. Rosenthal. Public key cryptography based on semigroup actions. *Advances in Mathematics of Communications*, No. 4 (Vol 1), 2007, pp. 489-507.

[20] Slavin, K. R. Public key cryptography using matrices. February 2007, *US Patent 10260818.*

[21] Atani, R. Public Key Cryptography Based on Semimodules over Quotient Semirings. *International Mathematical Forum 2*, no. 52, 2007, pp. 2561-2570.

[22] Atani, R., S. Atani, S. Mirzakuchaki. A Novel Public Key Crypto System Based on Semimodules over Quotient Semirings. IACR Cryptology ePrint Archive 2007:391.

[23] Dwivedi, A. et al. A Key-Agreement Protocol using Polynomials Root Problem over Non-Commutative Division Semirings. *International Journal of Computer Information Systems*, No. 3 (Vol. 2), 2011, pp. 60-69.

[24] Grigoriev, D., V. Shpilrain. Tropical cryptography. *Communications in Algebra*, vol. 42, issue 6, 2014, pp. 2624–2632.

[25] Durcheva, M., I. Trendafilov. Public Key Cryptosystem Based on Max – Semirings. *Appllied Math. in Engineering and Economics* - 38th Int. Conf., Sozopol, 2012, AIP Conf. Proc., vol. 1497, 2012, pp. 357-364.

[26] Durcheva, M. Public Key Cryptosystem Based on Two Sided Action of Different Exotic Semirings. *Journal of Mathematics and System Science* 4, 2014, pp. 6-13.

[27] Durcheva, M. An application of different dioids in public key cryptography, *Appllied Math. in Engineering and Economics* - 40th Int. Conf., Sozopol, 2014, in *AIP Conference Proceedings* 1631, 2014, pp. 336-343.

[28] Bezem, M. et al. Hard problems in max-algebra, control theory, hypergraphs and other areas. *Inf. Process. Letters*, 110(4), 2010, pp. 133-138.

[29] Akian, M. et al. Tropical polyhedra are equivalent to mean payoff games. *International Journal of Algebra and Computations*, 22(1), 2012, pp.1-43.

[30] Klauck H., Algorithms for parity games, in *Automata Logics, and Infinite Games*, v. 2500 of LNCS, pp. 553-563. Springer Berlin / Heidelberg, 20

[31] Aminu, A. On the solvability of homogeneous two-sided systems in max-algebra. *NNTDM* vol. 16, 2, 2010, pp. 5-15.

[32] Butkovič, P., M. MacCaig. On the integer max-linear programming problem. *Discrete Applied Mathematics* 162, 2014, pp. 128-141.

[33] Steiner, M. et al. Diffie-Hellman key distribution extended to group communication. in *Proceedings of the 3rd ACM Conference on Computer and Communications Security*, ACM: New York, NY, 1996, pp. 31-37.

[34] Steiner, M. et al. Key agreement in dynamic peer groups. in *IEEE Transactions of Parallel and Distributed Systems*, 11(8), 2000, pp. 769-780.

[35] Climent, J.-J. et al. Key agreement protocols for distributed secure multicast over the ring E_p^m. in *WIT Transactions on Information and Communication Technologies*, vol 45, 2013, pp. 13-24.

Information about the authors:

Mariana Durcheva is Assoc. Professor at the Faculty of Applied Mathematics and Informatics, Technical University of Sofia. Her research interests include Applied algebra, Discrete mathematics, Public key cryptography, Online education, Computer based education.

Malinka Ivanova is Assoc. Professor in the Department of "Electronics, Computer Systems and Technologies", College of Energy and Electronics, Technical University of Sofia. She is interested in eLearning, eAssessment, Technology-enhanced learning, Multimedia, Information security.

Manuscript received on 20 September 2017
Revised manuscript re-submitted on: 5 November 2017