Informatika a felsőoktatásban 2014 konferencia, Debrecen, 2014. augusztus 27–29.

A bilineáris leképezéseken alapuló hibrid mixnet alkalmazása az e-vizsga rendszerekben

Applying of the bilinear pairing based hybrid mix in e-exam systems

Kovács Zita[a]

[a]Debreceni Egyetem, Informatikai Kar
kovacs.zita@inf.unideb.hu

Absztrakt: Egy e-vizsgáztatási rendszer kidolgozásakor a szakembereknek igen körültekintően kell eljárni a biztonsági kérdéseket illetően. Míg hagyományos esetben például a személy azonosítására már jól kiforrott protokoll alkalmazható – fényképes igazolvány és a személy összevetése -, addig elektronikus esetben ez kriptográfiai építőegységek felhasználásával megoldandó feladat. Igényként jelent meg, hogy se a dolgozat írója, se a dolgozat javítója ne legyen ismert (azaz legyen anonim) a többi résztvevő előtt, így megadva a korrekt és kényszerítéstől mentes értékelés esélyét ezen résztvevők számára. Egy anonimitást megvalósító eszköz a mix network, melyet először Chaum írt le 1981-ben. Ezek hálózatba kötött szerverek, melyek egy üzenet küldőjét rejtik el. Az anonimitás mellett egyéb funkciók jelentek meg: küldhetünk választ az anonim feladó részére, s ha szükséges, akkor a lebonyolító szervezetek közösen felfedhetik az anonim küldők valódi azonosítóját. A mai gyakolatban egy vizsga esetén szükség van a résztvevők - vizsgázási, javítási - jogosultságának ellenőrzésére is. Feltétel lehet, hogy egy vizsgázó csak egy dolgozatot küldhessen be a határidőig vagy, hogy a vizsgát lebonyolító szervezet üzenhessen a vizsgázónak, (többkörös vizsga, pótlások/javítások kérése). Az eredmény beírásához tudni kell a vizsgázó azonosítóját, még akkor is, ha a vizsgázó nem akar hozzájárulni egy számára előnytelen értékeléshez. Ismerni kell a javító azonosítóját, a munka díjazásához, vagy ha reklamációra kell reagálnia. Az e-vizsga rendszerek készítésekor bevett szokás, hogy a különféle szolgáltatásokat megvalósító primitíveket ollózzák össze a rendszer megalkotói, így azonban biztonsági rések keletkezhetnek, s így támadhatóbb lesz a rendszer, még ha a primitívek igen megbízhatónak és erősnek is számítanak. A bilineáris leképezéseken alapuló hibrid mixnetünk éppen ennek a kiküszöbölésére is készült: úgy nyújt anonim szolgáltatást, hogy lehetőség van a korábban felvázolt egyéb igényeket is kielégíteni, úgy mint a résztvevők jogosultságának ellenőrzése, az anonim üzenetre való válaszolás, az anonim személy azonosítójának felfedése. A mixnet első a hibridek között, mely a kriptográfiailag igen jó tulajdonságokkal bíró bilineáris leképezésekre épít. A hibriditásnak köszönhetően hosszfüggetlen üzeneteket küldhetünk hatékonyan.

Kulcsszavak*:* hibrid mixnet, bilineáris leképezés, e-vizsga

Abstract: When we construct an electronic-exam (e-exam) system we should be taken of the security issues very carefully. While in the case of classic exams we have sofiticated protocols to identify an examinee – comparison of the person and his photo ID -, in the case of e-exams it is a problem to be solved using cryptographic primitives. Sometimes it is necessary that nor the examinee nor the corrector of the exam won't be known ie they are anonymous to the other participants. Because of this we can avoid bribery and subjective evaluation as well. In 1981 chaum proposed a mix network which provide anonymity. A mix network has several proxy server and it hides the sender of the message. After a while other functions have appeared besides anonymity: to send a reply to the anonymous sender, and if it is necessary we can reveal the real ID of the senders. In practical systems there is a need to verifying the eligibility of the participants. Even if the examinee is not cooperative then we still have to enter his bad grade. Another requirment is that for every examinee should send at most one examination paper till the deadline. Sometimes the study comittee wants to send a message to the anonymous examinee (multiround exam, supplement/correct request). Often when someone construct an e-exam system then he put together the cryptographic primitives thus formed vulnerabilities regardless how strong was the primitive. The bilinear pairing-based hybrid mixnet – proposed by A. Huszti and Z. Kovacs – eliminates these weak points because the optional functions such as eligibility verification of the participants, reply to an anonymous message, anonymity revocation are built in. This is the first hybrid mix which based on the bilinear

maps. The bilinear maps have really good properties and provide great services for three party protocols. Thanks for the hybrid property we can send efficiently long messages as well as short messages.

Keywords: hybrid mixnet, bilinear pairing, e-exam

1. Bevezetés

Az elektronikus oktatás azaz az e-learning elterjedésével az elektronikus vizsgáztató rendszerek kidolgozása kiemelt feladata a szakembereknek. Különféle igények jelentek meg, magától a vizsgától függően, s emellett a biztonsági követelmények teljesülését is garantálnunk kell. Hagyományos vizsgarendszerek esetén már sok-sok évnyi tapasztalat áll mögöttünk, kiforrott technikákkal rendelkezünk a vizsgafolyamat minden lépéséhez. Az elektronikus vagy e-vizsga esetén azonban szembetaláljuk magunkat a modern kor minden előnyével és hátrányával, így új ötletekkel és megoldásokkal kell előállnunk az egyes lépések megtételéhez, a különféle csalások kizárásához. Vizsgáról van szó mindkét – azaz hagyományos és elektronikus – esetben, azonban a rendszer kidolgozóinak teljesen más problémákkal kell szembenézniük az egyes esetekben. Elektronikus vizsgáztatáskor éppen a vizsga elektronikus mivoltát kihasználva szeretnének a vizsgázók előnyökre szert tenni, jogtalanul jegyet vagy jobb jegyet szerezni. Magyarországon még nem terjedt el, hogy egy e-vizsga az otthonunkból letehető legyen, hiszen akkor a vizsgázó helyett más is ülhetne a számítógép mellett. Amennyiben a vizsga mégis így történik, akkor a bizonyítványt bekérő munkáltató tisztában van ezen vizsga értékével. De gondolhatunk továbbképzésekre is, amikor nem cél tudás nélkül jegyet szerezni, mert azt a tudást utána használnunk kell. Ebben az esetben sem gond, hogy otthonról jelentkezik be a vizsgázó. Ettől függetlenül mi olyan vizsgakörnyezetet képzelünk el, amikor a vizsgázók összegyűlnek egy felügyelt helyen és ott vizsgáznak, azonban elektronikusan. Ilyen például a KRESZ vizsga, de az érettségit is ide gondolhatjuk, hiszen az iskolában letölthető a vizsga, de mégis felügyelet mellett vizsgáznak a tanulók. Természetes igényként merült fel, hogy a vizsgázók ne legyenek beazonosíthatók, s ezért általában név nélkül (másnéven anoniman), egy sorszámmal vagy pszeudonymmel vannak azonosítva az értékelés végéig. Amikor a kapott érdemjegy beírásra kerül, akkor derül ki, hogy melyik érdemjegy kihez tartozik. Ekkor azonban van olyan résztvevője a vizsgafolyamatnak, akiben meg kell bíznunk, hiszen bármikor elárulhatná, hogy egy adott pszeudonym kihez tartozik. Vannak olyan e-vizsga rendszerek (pl. [5]), amelyek úgy lettek megvalósítva, hogy senki se legyen megbízható résztvevő azaz megbíztható harmadik fél (angol teminológiával Trusted Third Party) nélküliek, mi is erre törekszünk. Érdekes elvárás, hogy a vizsgát javító személyek se legyenek ismertek az értékelés végéig. Mit érünk el ezáltal? Azt, hogy a tanuló nem tudja megkeresni a javítót, hogy megvesztegesse vagy megfenyegesse – közös néven kényszerítse – egy jobb jegy érdekében, hiszen nem tudja, hogy az ő dolgozatát ki fogja javítani. Ez persze akkor működik a valóságban is, ha nem egy tanár javít, hanem több. A biztonsági rendszerek építésekor feltételezzük, hogy a résztvevők minden csoportjában (vizsgázók, javítók) vannak megbízható felek, így ők bejelentenének egy ilyen megkeresést, tehát a tanulóknak nem éri meg találomra megvesztegetni a javítókat. Azt mondtuk, hogy a tanulók anonimak, nem a saját nevükkel dolgoznak, így, ha meg is találják az ő vizsgadolgozatukat javítót, hogyan mondják meg, hogy melyik dolgozatról van szó? Egyszerű a válasz, odaadják a pszeudonymjüket vagy ha ez nem megoldható, akkor egyszerűen olyan utalást tesznek a dolgozatban, ami által felismerhetővé válik, például az á betűről lehagyja az ékezetet háromszor egymás után vagy duplapontot tesz egy mondat végére. Sajnos előfordul a szubjektív értékelés is, hiszen emberek vagyunk azaz, hogy egyes javítók jobb vagy rosszabb jegyet adnának egy számukra kedvelt vagy nem kedvelt vizsgázónak, már ha tudnák, hogy melyik az ő dolgozata. Azzal, hogy nem ismert a vizsgázó,

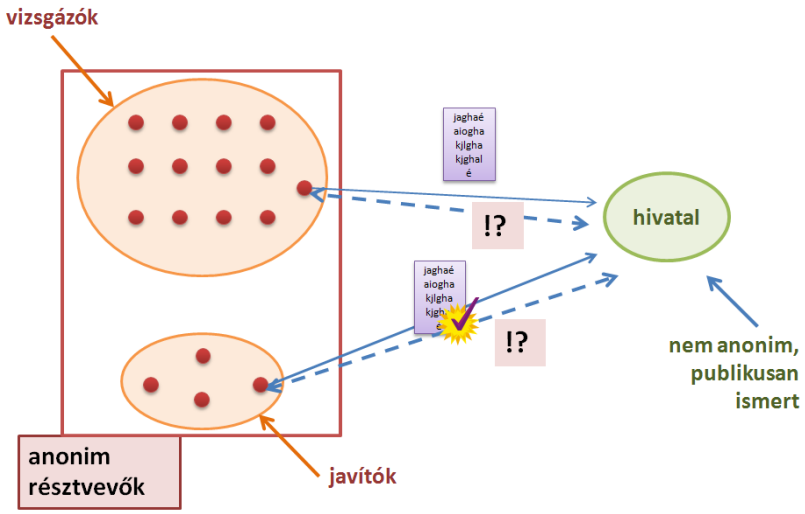
objektív értékelés válik lehetővé. Előfordulhat olyan eset is, amikor egy vizsga több körből áll, azaz az első rész elkészítése után kapja meg a második részt a vizsgázó, azaz miután benyújtott egy megoldást, várja a következő feladatsort. Ha ő anoniman vizsgázik, akkor nem tudjuk, hogy kinek kell válaszolnunk. A lényeg, hogy semmilyen azonosításra alkalmas lépés ne történjen a vizsgázás során, tehát nem azonosíthatja a vizsgázót az a számítógép, ahol ül, az első beküldött feladatsora, az üzenetienk egyike sem. A [2]-ben leírt hybrid mixnet megoldja ezt a kérdést, ők megvalósították az *anonim válasz* lehetőségét úgy, hogy rendszerükben nincs megbízható fél. Az ő rendszerük olyan, hogy folyamatos kommunikáció alakulhat ki egy anonim és egy nem anonim résztvevő között. Chaum 1981-ben javasolt egy új kriptográfiai eszközt [4], amelyet *mix networknek* nevezett el, az ő megoldásában egyetlen válaszra volt lehetőség. Lépjünk vissza egy kicsit. Mit értünk az alatt, hogy az egyik fél nem anonim. Az egyik fél, aki anonim az vagy a vizsgázó vagy a javító, akiknek ők üzenetet küldenek vagy akitől fogadnak, azok valamilyen hivatalok, akiknek nem szükséges anonimnak lenni, hiszen ők ismertek. Több funkciót is megvalósítanak a hivatalok: az egyik regisztrál, a másik kérdéseket küld, dolgozatokat fogad, értékelésre dolgozatot kiküld, értékelést fogad, végül regisztrálja a jegyet és a javítót. Az utolsó feladat azt is jelenti, hogy szükségessé válik megtudni, hogy kinek írja be az érdemjegyet/értékelést. Tehát egy bizonyos határidő után már az *anonimitást felfedjük*, hogy a vizsga eredményét rögzíteni tudjuk. A javító anonimitását is fel kell fednünk, hiszen a javított dolgozatok számától függ az ő fizetése. Az anonimitás visszahívását szintén megvalósítja a [2]-ben leírt hybrid mixnet. Továbbá [2]-ben belátták, hogy a mixnetük valóban teljesíti az anonimitást, az anonimitás visszahívását, az anonim választ, illletve korrektül működik. A mixnet azt is felkínálja, hogy csak *jogosult felhasználók üzenetét* vegye figyelembe a fogadó fél. Ezt a mixnetet felhasználva - a vizsgadolgozat beküldésétől - biztosíthatjuk, hogy elérjük az általunk is kívánt követelményeket. Némi módosítással azt is garantálhatjuk, hogy a vizsgát *egyszer* lehessen *beküldeni*. Vagy ha a vizsga olyan típusú, hogy a határidőig akárhányszor próbálkozhatnak a vizsgázók, akkor a legutoljára beküldött vizsgadolgozattot tekintjük érvényesnek. Ha jól megnézzük a felépített hybrid mixnet rendszert, akkor láthatjuk, hogy biztosítja a *letagadhatatatlanságot* is, azaz a vizsgázó és a javító nem tudja utólag letagadni, hogy az adott üzenetet ő küldte. Ebben a dolgozatban azt a kérdést szeretném felvetni, hogy hogyan lehetne megvalósítani a *globális és egyéni (azaz individuális) ellenőrizhetőséget*. Ezeknek lényege, hogy valaki valamit tudjon ellenőrizni. Azaz globális esetben akár egy külső szemlélődő is meggyőződhet arról, hogy a rendszer jól működik, a beküldött dolgozatokat kijavítják, a jegyet beírják. Az egyéni ellenőrzés az annyit takar, hogy minden vizsgázó, minden javító visszajelzést kaphat, s abból tudhatja, hogy a dolgozata/értékelése beérkezett, valóban az lett értékelve, valóban az az értékelés lett bejegyezve. Dreier és társai 2014-ben megvizsgáltak egy hagyományos és egy elektornikus vizsgát az ellenőrizhetőséget helyezve a középpontba [3]. Előtte el is készítették ezt az e-vizsga rendszert, melynek a Remark! nevet adták. Alapvető különbség, hogy más számítási modellen alapul, mint amit a hybrid mixnet használ, illetve az ő esetükben mindenkinek van tanúsítványa. Mi el szeretnénk kerülni ezt az igen költséges megoldást, tehát a széleskörű felhasználhatóságon kívül a költségre is odafigyeltünk. A hibrid mixnet épp ezért alkalmas számunkra, bilineáris párokon alapul, ami olyan költségmegtakarítást tesz lehetővé, mint az elliptikus görbék alkalmazása az utóbbi időben a kriptográfiában. A hybrid elnevezés mögött egy igen fontos tulajdonság bújik meg: tetszőleges hosszúságú üzenetet lehet hatékonyan kezelni, küldeni. Mindegy, hogy az üzenet egy szóból áll, vagy hosszabb kidolgozás, mindkét esetben a lehető legtöbb költség megtakarításra kerül. Általában egy rövid üzenet küldésekor kiegészítik “szeméttel” az üzenetet, hogy akkora legyen, amekkorát a rendszer megkíván, a hybrid esetben ilyesmire nincs szükség.

2. Alapfogalmak

2.1. Résztvevők

Az elektronikus vizsga résztvevői az alábbiak.
A **vizsgázó (V)** az a résztvevő, aki a tudásáról számot ad.
A **javító (J)** az a résztvevő, aki a vizsgázó által készített vizsgadolgozatot értékeli. A válaszok azon részét javítja ki, amely nem javítható automatikusan, szoftver által, például egy vizsga esetén fogalmazás javítása.
A **regisztrációs hivatal (R)** feladata, hogy a vizsgára jelentkezők és a javításra jelentkezők regisztrációját elvégezze, továbbá nyilvántartsa a rendszer jogosult felhasználóit. Ő ad aláírást, mellyel igazolja, hogy az adott üzenetet valóban egy jogosult felhasználó akarja elküldeni.
A **tanulmányi hivatal (T)** végzi a vizsga lebonyolítását, kiküldi a kérdéseket, összegyűjti a vizsgadolgozatokat, amelyeket javításra továbbít, majd begyűjti az értékeléseket. Szükség esetén kommunikál a vizsgázóval, javítóval. Rajta keresztül tud kommunikálni a vizsgázó és a javító is.
A **hirdetőtábla (HT)** egy olyan felület, amely bárki számára információkat szolgáltat, melyeket az arra jogosultak helyeznek el rajta. Az ellenőrzéseket a hirdetőtáblán lévő információk alapján tudják elvéezni az illetékesek.
A **mixszerverek (M_1, …, M_N)** olyan szerverek, melyek az anonim küldés szolgáltatást valósítják meg. Rajtuk keresztül történik a komminkáció, miközben az anonim felhasználók kilétét elrejtik. Az anonim felhasználók mindig valamelyik publikusan ismert hivatallal kommunikálnak, amely az utolsó mixszerver szerepét is betölti. A mixszereverek vesznek részt az anonimitás felfedésében is, a határidő lejárta után, közösen a tanulmányi hivatallal.

A vizsgázók és a javítók anonimak, a hivatalok nem anonimak. A vizsgázók és a javítók az tőlük elvárt üzeneteken (vizsgadolgozat, értékelés) kívül feltehetnek kérdést is egymás számára, amelyet a hivatalon keresztül küldenek el. Ezáltal kialakulhat egy ellenőrzött kommunikáció is, amennyiben a vizsga olyan, hogy erre lehetőséget kapnak a résztvevők. A résztvevők közötti kommunikációt az alábbi ábra szemlélteti (lásd 1. ábra). Amennyiben az *anonimitást* is igénybe vesszük, akkor az üzenetek a *mix szervereken keresztül* közlekednek.



1. ábra. E-vizsga résztvevőinek kommunikációi

2.2. Biztonsági kritériumok

Titkosság: A vizsgadolgozat, illetve az értékelés titkosak. Fontos, hogy bizalmas információk ne kerüljenek illetéktelenek kezébe.

Anonimitás: A vizsgázók és a javítók anonim módon vesznek részt a vizsgafolyamatban, kilétük nem ismert. Ezzel elérjük, hogy kényszerítésmentes, objektív értékelések történjenek.

Hitelesség: A kérdések, a válaszok és az értékelések hitelesek. Nagyon fontos elvárás, hogy biztosítsuk a hitelességet, vagyis, hogy a küldött információ a küldés során nem változott, illetve az információ valóban a küldőtől származik.

Egyszeri beküldés: Egy beküldött vizsgadolgozatot tekintünk érvényesnek. A vizsgázás során elkészített dolgozatot egyszer küldheti be a vizsgázó, ha többet is beküld a megadott határidőig, akkor az utoljára beküldöttet veszi figyelembe a rendszer, amennyiben olyan a vizsga menete.

Jogosultság: Csak az arra jogosultak vehetnek részt a vizsgán. Csak jogosult vizsgázó küldhessen be dolgozatot és csak jogosult javító küldhessen be értékelést. Külön érdekesség, hogy az anonimitás és a jogosultság együttesen kell teljesüljön, s ennek megvalósítása a regisztrációs hivatal által végrehajott bilineáris vak aláírás által történik.

Letagadhatatlanság: A vizsgadolgozat és értékelés beküldője ne tudja letagadni tettét, azaz, hogy ő volt az, aki az adott dokumentumot elküldte.

Egyéni és globális ellenőrizhetőség: Fontos követelmény, hogy minden résztvevő egyénileg tudja ellenőrizni, hogy az általa beküldött dolgozat/értékelés megfelelően lett-e feldolgozva, beleértve, hogy a vizsgázó, illetve a javító visszajelzést kap az adatok sikeres beküldéséről. A globális ellenőrizhetőség teljesül, ha egy külső megfigyelő is meggyőződhet arról, hogy szabályosan zajlott-e le a vizsga.

2.3. Bilineáris párok, hibrid mixnet

A [2]-ben leírt bilineáris párokon alapuló hibrid mixnetet és az általa nyújtott szolgáltatásokat alkalmazzuk az e-vizsgára, a mixnet az alábbi definícióra épít.

Definíció: Legyenek G_1 és G_2 két q rendű csoport, ahol q egy nagy prímszám. Egy $e : G_1 \times G_1 \rightarrow G_2$ leképezést **elfogadható bilineáris leképezés-**nek nevezünk, ha teljesíti az alábbiakat:

- *Bilineáris:* Egy $e : G_1 \times G_1 \rightarrow G_2$ leképezés bilineáris, ha $e(aP,bQ) = e(P,Q)^{ab}$ minden $P,Q \in G_1$ és minden $a,b \in Z_q^*$ esetén.
- *Nem-degenerált:* A leképezés nem minden $G_1 \times G_1$-beli párhoz rendel G_2-beli elemet identikusan. Mivel G_1, G_2 prímrendű csoportok, ha P generátora G_1-nek, akkor e(P,P) generátora G_2-nek.
- *Számítható:* Létezik hatékony algoritmus, mely kiszámítja e(P,Q)-t minden $P,Q \in G_1$-re.

A Weil és Tate pairing bizonyítja ilyen konstrukciók létezését. Tipikusan, G_1 egy elliptikus görbe csoport és G_2 egy véges test. Az ilyen leképezések bilineáris tulajdonsága adja a hibrid mixnetben a számítások, ellenőrzések alapját. Ezek a leképezések nagyszerű lehetőséget biztosítanak a háromrésztvevős protokollok kulcsmegosztásához, a három résztvevő titkos kommunikációjában. A 2000-es évek elejéig a Weil párokat elliptikus görbe rendszerek támadására használták, azonban 2000-től egyre több rendszerben ismerték fel a párok alkalmazásának előnyeit, például Joux, aki egy egykörös háromrésztvevős Diffie-Hellman protokoll elkészítésére használta [6]. Az egyes mixnetek különböznek például abban is, hogy

a mix szerverek milyen kriptográfiai műveletet végeznek, azaz titkosítanak, visszafejtenek, újratitkosítanak, vagy abban, hogy szimmetrikus vagy aszimmetrikus kriptográfiát alkalmaznak. A hibrid mixnet azért hibrid, mert épít mindkettőre, ezáltal éri el azt, hogy a tetszőleges hosszú üzenetek költséghatékonyan küldhetőek legyenek. Nekünk ez éppen megfelelő, mert vizsgáktól függően többféle hosszúságú üzenetet küldenek a résztvevőink. A dolgozat is lehet egészen kicsi, ha csak tesztről van szó, de kifejtős is, ami akár egész hosszúra nyúlhat. Az értékelés is lehet akár egy darab érdemjegy, míg az is lehet, hogy egy hosszabb szöveges értékelést készít és küld a javító.

3. Az e-vizsga

Tipikusan a vizsgák és az e-vizsgák lépéseit fázisokkal adják meg. A következő részben a javasolt e-vizsga **vizsgázó** szemszögéből tekintett fázisait írtuk le. A vizsgázó valamilyen képzésének végén (pl: önképzés, tanfolyam, egyetem) vizsgára jelentkezik. Ezt egy adott vizsga esetén megteheti például úgy, hogy kitölt egy formanyomtatványt, jelentkezik online. Egyszerű esetben a vizsgadíj befizetésekor máris jogosulttá válik a vizsgára. Személyes megjelenésével igazolja magát a regisztrációs hivatalnál, ezzel bekerül a vizsgára (illetve vizsgáztatásra) jogosultak adatbázisába. Ezután a vizsgázó megjelenik a korábban felvett vizsga időpontjában a felügyelt teremben, igazolja magát és helyet foglal. A kérdéseket megkapja, s elkezd dolgozni.

Előkészítő fázis Ebben a fázisban történnek meg az alábbiak: a rendszer nyilvános paramétereinek legenerálása, egyes résztvevők nyilvános-titkos kulcspárjainak legenerálása, a mix szerverek és a tanulmányi hivatal által megosztott kulcsok legenerálása, a vizsgadolgozat elkészítése (megj: a vizsga kérdéssorát valamilyen módon, akár nyilvánosan letölti a vizsgázó, majd elkészíti a dolgozatát, ehhez még nem szükséges az anonimitásnak teljesülnie)

Regisztrációs fázis A vizsgázó elkészült a dolgozatával, amit szeretne beküldeni a tanulmányi hivatal részére. Ehhez szüksége van egy hitelesítésre, amelyet a regisztrációs hivataltól tud megszerezni. A bilineáris vak aláírást használva eléri, hogy a vizsgadolgozatának kivonatán a regisztrációs hivatal aláírása szerepeljen.

Beküldés és keverés fázisa A vizsgadolgozat beküldéséhez a vizsgázó kiszámolja a szükséges értékeket és elkészíti a hibrid mixnet leírásában megadott üzenetét, majd elküldi azt az első mix szervernek. Az első mix szerver begyűjti a vizsgákat, majd ahogy a többi mix szerver kever és számol, majd továbbküldi az üzenetet a következő mix szervernek, végül utolsóként a tanulmányi hivatal fogja megkapni a vizsgázók üzenetét.

Fogadás fázisa Az utolsó mix szerver a tanulmányi hivatal, amely szintén végez számításokat, hogy megkapja a vizsgázó üzenetét. Ezután két ellenőrzést végez, melyekkel megbizonyosodik róla, hogy a vizsgázó jogosult volt beküldeni a dolgozatot, illetve, hogy az anonimitás felfedése megvalósítható lesz-e. Amennyiben a válaszok pozitívak, akkor a jogosult vizsgázóhoz bejegyzések kerülnek, az üzeneteit és néhány kiszámolt értéket tárolja el a tanulmányi hivatal.

Anonim válasz fázisa (opcionális) Ha további körök következnek, vagy valamilyen kérdés merült fel, vagy pótolnia kell valamit a vizsgázónak, akkor a tanulmányi hivatal válaszüzenetet fogalmaz meg, melyet az egyik tárolt érték alapján a mixszerverek kézbesíteni képesek az anonim vizsgázónak. Ez akár igény szerint többször is megtörténhet.

Anonimitás visszahívása A vizsga (vizsgázás és értékelés) végeztével szükség van az értékelés rögzítésére, így az anonim vizsgázó kilétét felfedi közösen a tanulmányi hivatal és a mix szerver. Ha a vizsgázó együttműködik, akkor lehetőség van költségmegtakarításra, mert ebben az esetben jóval gyorsabban és hatékonyabban felfedhető a valódi azonosító.

Láthattuk, hogy a fázisok során mindvégig a vizsgázóra összpontosítottunk. A **javító** esete is pontosan így zajlik. A tanulmányi hivatal a vizsgadolgozatok értékelését megkezdi egy adott időpontban, vagy akár rögtön a vizsga után. A jogosult vizsgázókat nyilvántartja a regisztrációs hivatal. A vizsgajavításkor a tanulmányi hivatal valamilyen véletlen sorsolással kiosztja a dolgozatokat a javítók között (akárcsak a vizsgázók esetén a kérdéseket), akik elvégzik a javítást. Az értékelés beküldéséhez futtatják az előbb leírt *regisztrációs és beküldés és keverés fázisokat*, így eljuttatva az értékelést a tanulmányi hivatalnak, anonim módon. Ha már nem merül fel egyik oldalról sem kérdés és nem hamarabb, akkor elindulhat az *anonimitás visszahívása fázis*, mind a vizsgázók, mind a javítók személyére vonatkozóan.

4. Biztonsági értékelés

Az *egyszeri beküldés* és az *egyéni és globális ellenőrizhetőség* kritériumok kivételével az összes többit biztosítja az alkalmazott hibrid mixnet. Ezért a két kivétellel fogunk foglalkozni.

Az egyszeri beküldés követelményét úgy tudjuk teljesíteni, hogy a tanulmányi hivatal egy vizsgadolgozat fogadásakor ellenőrzi, hogy adott vizsgázó nem küldött-e már be dolgozatot. Ha többszöri is küldhet be dolgozatot, melyek körül az utolsó az érvényes, akkor felülírjuk a tárolt dolgozatot. Mivel a vizsgázó hitelesítést egyszer kérhet a regisztrációs hivataltól (ezt a hivatal tudja kezelni, hiszen a hitelesítéshez elküldi a saját azonosítóját a vizsgázó), így a μ_i érték azonosítja a dolgozatot, vagyis a tanulmányi hivatal ki tudja keresni, hogy szerepel-e már ilyen érték az adatbázisában, azaz a vizsgázó küldött-e már be dolgozatot. Tehát ezen követelmény teljesjülését a hibrid mixnet protokolljának egy kis módosításával elérhetjük, ha a tanulmányi hivatal ezt a plusz ellenőrzést beiktatja.

Az egyéni és globális ellenőrizhetőség teljesüléséhez a [3]-ban leírt fogalmakat tekintem alapul. Az egyéni ellenőrzést a vizsgázó szempontjából tekintjük, s az alábbiakat jelenti. Minden vizsgázó szeretné ellenőrizni, hogy a vizsgadolgozata korrektül lett értékelve. Ez jelenti azt, hogy a neki kiküldött kérdések hitelesek, az őáltala beküldött dolgozatot elfogadta a tanulmányi hivatal és azt értékelésre megkapta egy javító, értékelte a dolgozatát egy javító, a kapott értékelés korrekt, a dolgozatra adott értékelést valóban a dolgozat készítője kapja meg, a vizsgázót értesítik a kapott értékelésről. A globális ellenőrizhetőség egy külső résztvevő által történik, s az alábbiakat takarja. Csak jogosult vizsgázók által beküldött dolgozatokat tárolja a rendszer, minden jogosult vizsgázó által beküldött dolgozat és csak ezek vannak kiküldve javításra, valamint ezek vannak értékelve, csakis ezek a dolgozatokra kapott jegyek vannak figyelembe véve. Ezen ellenőrizhetőségek (egyéni, globális) teljesülését többféle módon tudjuk belátni. A [3]-ban Proverif technikát alkalmazva szeretnénk megvizsgálni a mi esetünkben mennyire teljesülnek, illetve milyen módosítással teljesülnének ezek a feltételek. Jelenleg még annyit mondhatunk, hogy az egyéni ellenőrzések némi módosítás után könnyen teljesülnek, úgy mint a tanulmányi hivatal a vizsgadolgozat beérkezésekor egy visszaigazolást küld a hirdetőtáblára, aminek a segítségével a vizsgázó megbizonyosodhat róla, hogy a dolgozat beérkezett, stb. Ezen megoldásokat bemutattuk már egy korábbi dolgozatunkban, 2011-ben [1]. A hibrid mixnet működése olyan, hogy biztosítja

a jogosultság folyamatos ellenőrzését, ezért a globális ellenőrizhetőség egyes részei szintén teljesülnek. Ennek a formális leírása, Proverif alkalmazás a következő feladatunk, terveink között szerepelnek.

5. Összefoglalás

A dolgozatban felvázoltunk egy olyan e-vizsgát, amely a [2]-ben leírt bilineáris leképezéseken alapuló hibrid mixnetet alkalmazza a dolgozatok és értékelések beküldéséhez, aholis szükség van a küldő felek anonimitásának biztosítására. A mixnet által bizosított szolgáltatások éppen azok, amelyekre az e-vizsga rendszerekben is szükség van. Námi módosítással mindenféle egyéb speciális igény (egyszeri beküldés, ellenőrizhetőségek) teljesülését garantálhatjuk. Az egyéni és globális ellenőrizhetőséget részletesebben körül fogjuk járni, mivel vannak már ehhez használatos módszerek, azokat alkalmazzuk. A [3]-ban leírt e-vizsga hasonlóan működik, viszont a miáltalunk bemutatott rendszer költségmegtakarítást is lehetővé tesz. Terveink között szerepel ebből a szempontból történő összehasonlításuk is.

6. Köszönetnyilvánítás

A publikáció elkészítését a TÁMOP-4.2.2.C-11/1/KONV-2012-0001 számú projekt támogatta. A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg. Továbbá szeretnék köszönetet mondani Dr. Huszti Andreának kutatásaink során tett segítő megjegyzéseiért, munkájáért és odaadó támogatásáért.

Irodalomjegyzék

[1] Huszti Andrea és Kovács Zita: Univerzális kriptográfiai protokoll e-felmérésekhez, *Informatika a felsőoktatásban Konferencia Kiadványa*, Debrecen, (2011), 592--600.

[2] Huszti Andrea és Kovács Zita: Bilinear Pairing-based Hybrid Mixnet with Anonymity Revocation, *(megjelenés alatt)*

[3] J. Dreier, R. Giustolisi, A. Kassem, P. Lafourcade, G. Lenzini: On the Verifiability of (Electronic) Exams, *Verimag Research Report* n^0, Grenoble, (2014)

[4] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, *Commun. ACM 24(2)*, (1981), 84-88.

[5] Huszti Andrea és Pethő Attila: A secure electronic exam system, *Publ. Math. 77/3-4* Debrecen, (2010), 299-312

[6] A. Joux: A One Round Protocol for Tripartite Diffie-Hellman, *Algorithmic Number Theory, 4th International Symposium, ANTS-IV Leiden, The Netherlands, July 2-7, 2000, Proceedings, LNCS 1838*, (2000) ,385-393