Bioszkript alkalmazása az elektronikus szavazásban

Jungbauer Alexandra — Somogyi Tamás*

Budapesti Műszaki és Gazdaságtudományi Egyetem
Gazdaság- és Társadalomtudományi Kar
Információ- és Tudásmenedzsment Tanszék
1111 Budapest, Sztoczek u. 2. St. ép. I. em. 117.
Telefon: (36 1) 463-1832, Fax: (36 1) 463-4035
email: jungbauer@vnet.hu, somogyitl@freemail.hu

Absztrakt

A tanulmány két olyan, a szerzők által kidolgozott elektronikus szavazási rendszer koncepcióját ismerteti, amely a biometrikus rejtjelezés, technikailag a bioszkript alkalmazásán alapul. Az ismertetett rendszerek lényege, hogy nem központilag tárolt, személyazonosításra alkalmas biometrikus azonosítók (például ujjlenyomatok) használatán alapulnak, hanem a szavazásra jogosultak biometrikus adataiból származtatott és így harmadik személyek számára értelmezhetetlen, de a szavazási jogosultságot egyértelműen bizonyító bioszkript használatán. Ezzel biztosíthatók a képviselőválasztások és népszavazások titkossági, biztonsági és egyéb alapvető feltételei, azzal a külön előnnyel, hogy a leírt rendszerek alkalmazásával magas szinten teljesíthetők a személyes adatok védelmének jogi és technológiai követelményei, kiemelten a célhozkötöttség, vagyis az adatkezelési célhoz szükséges és elégséges mértékű és időtartamú adatkezelés biztosítása.

Kulcsszavak: *bioszkript, elektronikus szavazás, ujjlenyomat, biometrikus rejtjelezés*

1. Bevezetés

A demokrácia lényege, hogy az emberek a sorsukról, jövőjükről, az ország és szövetségi rendszere életéről választott képviselőik útján dönthessenek, az igazán fontos kérdésekről pedig személyesen nyilváníthassanak véleményt. A modern képviseleti demokráciákban a képviselők (helyi önkormányzati vagy országgyűlési képviselők) jelölését és megválasztását egységes alapelveket tükröző választási eljárásban, illetve az azokat tartalmazó jogszabályokban határozzák meg. A választások lényege, hogy a pártok és jelöltek között a választópolgárok szabad akaratuk szerint dönthessenek. Népszavazást sok

* Jungbauer Alexandra és Somogyi Tamás a BME végzős műszaki informatikus hallgatói, a GTK Információ- és Tudásmenedzsment Tanszék tudományos diákköri pályázói.

mindenről, szinte bármikor lehet tartani (pontosan lásd később). A szavazásokon, választásokon való részvétel nem kötelező, az a választópolgár szabad elhatározásán múlik.

Noha a választások egy bonyolultabb eljárásban csupán a képviselők személyének meghatározására irányulnak, a népszavazások pedig egyszerűbb eljárásban a közvetlen véleménynyilvánításra, mind a kettőnél alapvető fontosságú az eljárás tisztaságának megóvása, ellenőrizhetőségének biztosítása, a csalás megakadályozása.

Ugyanilyen fontos, hogy a választások és a népszavazások eredménye a választópolgárok *mint közösség* akaratát tükrözze, vagyis az egyéni vélemények összességét, és ne magukat az egyéni véleményeket. Az a tény, hogy egy szavazásra jogosult kire kíván szavazni, ténylegesen kire szavazott, vagy szavazott-e egyáltalán, kizárólag az érintett szavazó magánügye. A személyes adatok feletti önrendelkezés alkotmányos joga erre is kiterjed: a választópolgár maga dönti el, hogy véleményét, szavazatát más tudomására hozza-e. A szavazási rendszernek azonban alapvető feladata, hogy a szavazatok és a szavazók között ne lehessen semmilyen kapcsolatot teremteni, erre még a választópolgár se legyen képes. Ez az egyik garanciája annak, hogy a választók illetéktelen befolyástól mentesen, szabad akaratukból nyilvánítanak véleményt.[1]

Informatikai szempontból (ha eltekintünk a jelöltállítás, a jogorvoslat stb. folyamatától) mind a két aktus hasonló követelményeket támaszt a lebonyolítóval szemben, akár képviselőjelöltre vagy pártra, akár népszavazáson feltett kérdésre történik a szavazás, ezért a következőkben mi sem teszünk különbséget képviselőválasztás és népszavazás között.

Már a mai népszavazásokban, választásokban is jelentős szerepet játszik az információs technológia, elsősorban a szavazatok összesítésében és továbbításában. A technológia fejlődése azonban lehetővé tette a tisztán elektronikus úton lebonyolítható szavazások megvalósítását is. A számos lehetséges megoldás közül néhányat a gyakorlatban is kipróbáltak, megbízhatóságukról, alkalmazhatóságukról azonban megoszlanak a vélemények.

Tekintettel az elektronikus szavazásoknál biztosítandó adatvédelmi és adatbiztonsági követelményekre (melyek összhangban vannak a papír alapú szavazás követelményeivel), megvizsgáltuk, hogy az adatalanyok védelmére kifejlesztett ún. PET technológiák egyike, a biometrikus rejtjelezés (a bioszkript) hogyan alkalmazható az elektronikus szavazásokban.

[1] A személyes adatok feletti önrendelkezést ugyanakkor maga a választási eljárás is korlátozza, például a választói névjegyzék összeállításánál, illetve közszemlére tételével, de ez a korlátozás összhangban van a választások alkotmányos céljával.

E tanulmányban két, saját elképzelésen alapuló, bioszkriptet alkalmazó elektronikus szavazórendszert mutatunk be és igazoljuk, hogy eleget tesznek az elvárható biztonsági és adatvédelmi követelményeknek.

2. Szavazás, választás

Magyarországon a választójoggal rendelkezők négyévente választják az őket helyi és országos szinten képviselő politikusokat. Az Alkotmány rögzíti, hogy milyen feltételekkel és milyen kérdésekben lehet országos népszavazást tartani, illetve, hogy a szavazás mikor eredményes. Szintén az alaptörvény foglalkozik azzal a kérdéssel is, hogy ki vehet részt a szavazásokon.

A választópolgárok nyilvántartásáról a választási eljárásról szóló 1997. évi C. törvény rendelkezik:

„12. § A helyi választási iroda vezetője a választás kitűzését követően a személyiadat- és lakcímnyilvántartás adatai és a választójoggal nem rendelkező nagykorú polgárok nyilvántartása alapján szavazókörönként összeállítja a választójoggal rendelkező polgárok névjegyzékét, és azon a változásokat folyamatosan átvezeti.

13. § (1) A névjegyzékbe fel kell venni azokat a választójoggal rendelkező személyeket, akiknek a lakóhelye, ennek hiányában tartózkodási helye (a továbbiakban: lakcím) a szavazókörben van.

(2) A névjegyzéket úgy kell összeállítani, hogy alkalmas legyen a főváros, a megye, a település, illetőleg a választókerület, a szavazókör és a választópolgár azonosítására. A névjegyzék tartalmazza a választópolgár:

a) családi és utónevét (nők esetén leánykori családi és utónevét is),
b) személyi azonosítóját,
c) lakcímét,
d) névjegyzékbeli sorszámát,
e) az azonos nevű és lakcímű választópolgárok születési idejét, ennek azonossága esetén egyéb természetes személyazonosító adatát.”

A választói névjegyzéket közszemlére kell tenni. A választópolgároknak választási értesítőt kell kapniuk. Ha nem kapnak, vagy kettőt kapnak, azt azonnal jelezniük kell. A választási értesítő egyfelől igazolás, hogy a választópolgárt felvették a választói névjegyzékbe, másfelől innen tudja meg, hogy hol és mikor szavazhat.

A választás napján a szavazatszámláló bizottság a legelső szavazó jelenlétében megnézi, hogy üres-e az urna, és az ellenőrző lap aláírása után az urnát lepecsételi. A szavazatszámláló bizottság minimum háromfős. A bizottság egyik fontos feladata a választópolgárok személyazonosságának az ellenőrzése, ezt még a leghosszabb sor esetén is meg kell tenniük. Így biztosítják, hogy csak a választói névjegyzéken szereplők, és mindenki legfeljebb egyszer szavazhasson. A szavazólapok átvételét mindenki az aláírásával igazolja. A szavazólapokat a választópolgár szeme előtt kell lepecsételnie a bizottságnak, az előre lepecsételt lapokat senki sem köteles felhasználni. Ezek után mindenki a szavazófülke magányában, alapos megfontolás után szavaz, majd a szavazólapját egy borítékban a bizottság szeme láttára az urnába dobja.

A választás során tehát mindenki szabad akarata szerint, csak egyszer szavazhat, és biztos lehet abban, hogy senki sem fogja megtudni, hogyan szavazott. A választási csalás a magyar választási eljárás szabályai alapján „lehetetlen", ha a választás résztvevői a törvényi rendelkezések betartásával ügyelnek a választások tisztaságára.

2.1. Elektronikus szavazás, gépi szavazás

Elektronikus szavazás alatt olyan szavazást értünk, amelyben számítógépeket, elektronikus berendezéseket használnak a szavazatok rögzítésére és számlálására.[2] Elektronikus úton lehet szavazni telefonon, az interneten keresztül, sms-ben, esetleg kábeltévén keresztül. (A postai úton történő szavazást papír alapúnak tekintjük, csakúgy, mint a mai, hagyományos szavazást.) A telefonon, mobiltelefonon keresztüli szavazást manapság a közvéleménykutató cégek preferálják. Nekik nem olyan fontos az azonosítás, számukra elég, ha azt tudják, hogy az alany milyen csoportba tartozik (pl. 18–25 év közötti tanuló).

Az elektronikus szavazás egyik fő célja a szavazási eljárás gépesítése, automatizálása. Mechanikus szavazógépeket 1892 óta (a mai napig is) használnak az Amerikai Egyesült Államokban. Minden jelöltnek van egy ilyen gépe. A gépen egy kar található, ha ezt meghúzza a szavazó, akkor a gép belsejében a számláló értéke eggyel nő. A szavazás végén a gépek belsejében lévő számlálók értékét a hivatalnokok leolvassák. Ezen gépek hátrányai: nincs naplózás, a gépek nagyok és nehezek, a kar sérülése, a fogaskerekek kopása miatt nem érzékelhetnek minden szavazatot.

A szavazógépek egy másik fajtáját a kártyás rendszerek alkotják. A szavazólap szerepét egy kártya tölti be. A jelölt neve mellett a kártyát ki kell lyukasztani. A lyukas kártyákat

[2] A szakirodalom nem egységes az elektronikus szavazás meghatározásában. Egyesek csak azt értik ez alatt, amikor minden lépés elektronikus úton történik.

összegyűjtik és gépekkel megszámolják. A gépbe helyezett kártya két oldalán érzékelők vannak; ahol lyuk van, ott az érzékelők összeérnek és záródik egy áramkör, ami léptet egy számlálót. Egyszerű használni, de oda kell figyelni, hogy pontosan hol lyukasztja ki a kártyát a szavazó.

Optikaiolvasó-rendszerek. A szavazók a szavazólapon a jelölt neve mellé jelet rónak, rajzolnak, ezeket a jeleket a rendszer megkeresi a lapon és felismeri. Vigyázni kell, hogy a szavazó pontosan, a megfelelő helyre rajzoljon. Ma az USA államainak mintegy 40 százalékában használnak ilyen gépeket.

Léteznek olyan rendszerek is, amelyek azonnal továbbítják a szavazatokat (DRE — Direct Recording Electronic voting machines). Itt a szavazók billentyűzeten vagy érintésre érzékeny monitorokon keresztül nyilváníthatnak véleményt, tehát már nem használnak papírt és tollat.[3]

2.1.1. A jó elektronikus szavazórendszerrel szemben támasztott követelmények

Az elektronikus szavazási rendszerek, koncepciók áttekintésénél azzal szembesültünk, hogy más-más, egymást részben átfedő feltételrendszerek teljesítését igényelték a különböző rendszerek. Álláspontunk szerint a következő feltételeket minden elektronikus szavazási rendszernek maradéktalanul teljesítenie kell:

1. Pontosság — a szavazatokat ne lehessen utólag módosítani, és kizárólag az érvényes szavazatokat vegye figyelembe a rendszer.
2. Demokratikusság — minden szavazójoggal rendelkező személy szavazhasson, csak ők szavazhassanak, és mindegyikük csak egyszer.
3. Titkosság — senki, sem a szavazók, sem a szavazás lebonyolításában részt vevők ne tudhassák meg, hogy ki kire vagy mire szavazott, ennélfogva egyetlen szavazó se tudja később igazolni, hogy ő kire vagy mire szavazott. Ez a feltétel azt biztosítja, hogy mindenki idegen befolyástól mentesen szavazhasson, vagyis ne lehessen szavazatot vásárolni, vagy fenyegetéssel befolyásolni a szavazókat, választókat.
4. Ellenőrizhetőség — az előző feltétel betartása mellett bárki igazolhassa, hogy a szavazatokat korrektül számolta össze a rendszer. Egyesek szerint elég, ha ezt csak egy bizottság tudja igazolni.

[3] Lásd Lorrie Faith Cranor Voting After Florida: No Easy Answers című, 2001. március 19-én kelt cikkét. (http://lorrie.cranor.org/voting/essay.html)

5. Egyszerűség — a szavazók a lehető legegyszerűbben szavazhassanak, vagyis a rendszer használatához ne kelljen semmilyen képzettség, számítástechnikai ismeret vagy különösebb gondolkodási képesség.
6. Rugalmasság — bonyolultabb, összetett kérdést is fel lehessen tenni, és a szavazók ne csak egy szóra (például igen/nem) szavazhassanak.
7. Mobilitás — a rendszer ne függjön a szavazás helyszínétől; minden választókerületben és szavazóhelyiségben egységes rendszer legyen.
8. Gyorsaság — a lehető leghamarabb nyilvánosságra lehessen hozni a pontos végeredményt.

Ezeket a feltételeket a mai magyarországi választási rendszerek teljesítik, így a demokratikusságot a választói névjegyzék összeállítása és kezelése, a pontosságot és titkosságot a szavazóhelyiségek kialakítása és a szavazatszámlálási bizottságok működése, az ellenőrizhetőséget a szavazatok korlátozott időn belüli újraszámlásásának lehetősége, a gyorsaságot pedig a jelenlegi szavazatösszesítő rendszerek működtetése biztosítják.

2.1.2. Az elektronikus szavazás résztvevői

Vannak egyfelől a szavazók, másfelől a szavazás lebonyolításában segédkezők. Ez utóbbiak azok,

a) akik a szavazóhelyiségben látnak el feladatokat, nevezzük őket adminisztrátoroknak;
b) akik a szavazóhelyiségeket és a központot összekötő hálózatot felügyelik;
c) akik a számítógépek programjait írták;
d) akik a szavazás lebonyolításában segédkező gépeket készítették.

Manapság az összes felsorolt résztvevő megtalálható a választásokon, hiszen a szavazóhelyiségek már most is összeköttetésben állnak a központi választási irodával, és a szavazatok feldolgozásában már most is segédkeznek számítógépek.

Szavazásnál mind a szavazóknak, mind a szavazás lebonyolításában segédkezőknek azonosítaniuk kell magukat. Elektronikus szavazásnál ezt a legegyszerűbben egy intelligens kártyával tudják megtenni, amely valamilyen egyedi azonosító adatot tartalmaz. Lehetséges kártya helyett jelszó használata is, esetleg jelszóval (is) védett kártya. A szavazók azonosítása már a szavazás előtt is megtörténhet, a kártya átvételekor. Elképzelhető, hogy egyáltalán nincs kártya, ekkor a szavazóhelyiségben a szavazó a személyi igazolványát mutatja fel. A szavazás lebonyolításában részt vevő személyeknek mindenféleképpen igazolniuk kell magukat a rendszernek. Nekik kell kártya, jelszó.

2.1.3. Támadások[4]

Támadásról akkor beszélünk, ha valaki vagy valakik megpróbálják a választások eredményét befolyásolni, vagy a szavazás titkosságát megsérteni, vagy a szavazás menetét megakasztani.

Lehetséges támadások:

1. Többszörös szavazás, vagyis ha egynél többször szavaz valaki. Erre a támadásra akkor képes a választó, ha a kártya túl egyszerű. Ekkor ugyanis készíthet több kártyát is, és ezekkel megpróbálhat szavazni.
2. Adminisztrátori jogokkal való visszaélés (a szavazás kezdetének elhalasztása, vagy éppen a szavazás lezárása stb.). A választó is támadhat így, ha sikerül egy adminisztrátori kártyát hamisítania, és képesek erre a támadásra a gépek és programok készítői is, ha előre elrejtenek egy ilyen utasítást a rendszerben.
3. A rendszer módosítása úgy, hogy az ne működjön helyesen, például ne vegyen figyelembe minden szavazatot, jegyezze meg, hogy ki kire szavazott stb. E csalással a rendszer készítői próbálkozhatnak, például ha nem a nekik tetsző eredmény várható.
4. Legális szavazat törlése, módosítása, vagy legálisnak látszó szavazat készítése (például ha a programkódban szerepel egy olyan utasítás, hogy minden harmadik szavazatot, amelyet „A” párt kapott, adjon hozzá a „B” párt szavazataihoz, és a „C” párt szavazatait érvénytelenítse). A hálózatot felügyelőkkel is vigyázni kell, mert esetleg nem engednek továbbhaladni minden üzenetet a hálózaton, vagy módosítják azokat.
5. A szavazólap módosítása, például a pártok és jelöltjeik nevének felcserélése, és így a választók megtévesztése. A rendszer készítői képesek erre.
6. Egy szavazat és a hozzá tartozó szavazó nevének felfedése. Ugyancsak a rendszer készítői támadhatnak így.

Mindezek mellett a szavazóhelyiség munkatársai is képesek a felsorolt támadások végrehajtására, hiszen adminisztrátori kártyáik több jogot biztosítanak számukra.

[4] A támadások számbavételénél Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin és Dan S. Wallach Analysis of an Electronic Voting System című, 2003. július 23-án megjelent cikkére támaszkodtunk. (http://avirubin.com/vote.pdf)

A támadások megelőzésére, az ellenük való védekezésekre most nem térünk ki, de hangsúlyozzuk, hogy egy elektronikus szavazórendszer tervezésekor és felügyeletekor erre gondot kell fordítani.

Ugyancsak hangsúlyozzuk, hogy az elektronikus berendezések helytelenül is működhetnek, tönkremehetnek. Egy gép leállása, meghibásodása vagy áramszünet esetén nem szabad előfordulnia annak, hogy egy szavazóhelyiséget be kelljen zárni, a szavazásnak tovább kell folynia, vagy egy másik gépen, vagy papír és toll segítségével. Ráadásul nagyon fontos, hogy ha éppen egy szavazat leadása közben romlik el valami, akkor az érvényes szavazat ne vesszen el. Az is fontos, hogy a hálózat megbízható legyen, illetéktelenek ne férhessenek hozzá, és a hálózati összeköttetés megmaradjon rendkívüli körülmények között is.

2.1.4. Protokollok

Az elektronikus szavazási protokollokat az alábbiak szerint csoportosíthatjuk:[5]

1. *Egyszerű protokoll* — a szavazó a szavazatát és az azonosítóját odaadja egy ellenőrnek, aki az azonosító alapján megnézi egy listán, hogy a szavazónak van-e joga szavazni, és ha minden rendben, akkor a szavazatát továbbítja a szavazatszámlálónak, a szavazót pedig kihúzza a listájáról. Az ellenőr és a szavazatszámláló természetesen lehet elektronikus gép, és mindkettő lehet a szavazóhelyiségben lévő gépen is megtalálható, de lehet a központban is. Ez egyszerű, könnyen megvalósítható protokoll, sajnos, több hibája is van. Ha valaki nem a saját azonosítóját használja, akkor esetleg többször is szavazhat, és a szavazó nem bizonyosodhat meg arról, hogy a szavazatát elfogadta a rendszer. Természetesen a rendszer tervezőinek a feladata megteremteni a biztonságos és megbízható kommunikációs csatornát a szavazatszámláló és az ellenőr között.

2. *Két ügynök protokoll* — az ellenőr minden szavazónak ad egy egyedi azonosítót, és az azonosítók listáját elküldi a szavazatszámlálónak. A választó szavazáskor két dolgot küld el a számlálónak: az azonosítót és kódolva az azonosítót a szavazattal. A számláló visszaküldi a kódolt fájl másolatát, így igazolva a szavazónak, hogy a szavazata időben, módosítatlanul megérkezett. A szavazó ezek után elküldi a kulcsát, aminek a segítségével a számláló dekódolja a fájlt. Megnézi, hogy az eredetileg kódolatlanul kapott azonosító és a

[5] A protokollok leírásánál Lorrie Faith Cranor Electronic Voting — Computerized polls may save money, protect privacy című, az ACM Crossroads Student Magazine-ban 1996-ban megjelent írását, valamint Farrel Lifson The Security of Electronic Online Voting című munkáját vettük alapul (http://people.cs.uct.ac.za/~flifson/things/security/essay.html).

dekódolt azonosító egyezik-e, és rajta van-e a listán, amit az ellenőrtől kapott. Ha vége a szavazásnak, akkor a számláló közzétesz egy listát, melynek elemei párok. A pár első része egy szavazat, a másik fele pedig a hozzá tartozó kódolt fájl. A szavazó így ellenőrizni tudja, hogy szavazatát helyesen, akaratának megfelelően figyelembe vették. Sajnos, itt is figyelni kell néhány dologra. Ha az ellenőr és a számláló összejátszik, akkor a szavazás titkosságának vége. Másrészt, ha a választó be tudja bizonyítani, hogy hogyan szavazott, akkor a szavazatokat pénzzel vagy erőszakos fenyegetéssel meg lehet szerezni. Egy megjegyzést még tennünk kell a kódolásról. Fontos, hogy senki se tudja dekódolni a kulcs nélkül a kódolt fájlt. Ma már léteznek ilyen egyszer használatos, nagyon nehezen feltörhető kódok, így ezzel a továbbiakban nem foglalkozunk. Van ennek a protokollnak egy másik változata is, az *„egy ügynök protokoll”,* amikor az ellenőr és a számláló feladatát ugyanaz a szereplő látja el.

3. *Borítékolt protokoll* — ez a protokoll használatos elektronikus kereskedelemben is. A lelke a borítékolás[6]. A szavazó a szavazatát kódolva és borítékolva elküldi az ellenőrnek. Az ellenőr megnézi, hogy a szavazó jogosult-e a véleménynyilvánításra, és ha igen, akkor aláír egy igazolást. A borítéknak az a szerepe, hogy az ellenőr ne láthassa a kódolt szavazatot. A szavazó ezek után elküldi a számlálónak a kódolt szavazatát és az ellenőr igazolását, de boríték nélkül. A számláló megnézi az ellenőr aláírását, hogy valódi-e. A protokoll működése egy egyszerű matematikai problémára épül. Két számot, elég nagy számot a mai tudásunk szerint egy pillanat alatt össze lehet szorozni. Viszont egy elég nagy számnak a prímtényezős felbontása már reménytelen próbálkozás lenne. A protokoll lépései a következők:

   a) Az ellenőr minden szavazásra jogosult szavazónak küld egy egyedi azonosítót.
   b) A szavazás napján a választó eldönti, hogyan szavaz [sz], majd kódolja a szavazatát [c(sz)], és megszorozza egy számmal [c(sz)*p]. Ezt, és az azonosítóját elküldi az ellenőrnek.
   c) Az ellenőr megnézi az azonosító alapján, hogy a szavazó jogosult-e szavazni. Ha igen, akkor küld a szavazónak egy igazolást [d]. Ez annyit tartalmaz, hogy a c(sz)*p egy legális szavazat.

[6] Eredetiben: *blinding.* Az úgynevezett vak aláírás protokollnál használt eljárás (bővebben lásd Tóth Csaba „Egy ideális anonim digitális pénzrendszer” című tanulmányában), amit egyes magyar források vakításnak, sőt „vakolásnak” fordítanak. A magyar szakirodalomban javasolt „borítékolás” fogalomról lásd még Székely Iván: PET technológiák: a személyes adatok védelmének korszerű eszközei. (In: *Létezik-e adatvédelem adatbiztonság nélkül?* Infoszféra Kft., Budapest 2000.)

d) A szavazó a számlálónak elküldi az igazolást [d], és a c(sz)-t, valamint a p-t. A számláló ezek alapján el tudja dönteni, hogy a c(sz) egy legális szavazat-e. Ha igen, akkor
e) A számláló a c(sz)-t visszaküldi a szavazónak, igazolva, hogy a szavazatát regisztrálta. Az is előfordulhat, hogy nem a szavazónak küldi el, hanem egyszerűen az urnazárás után közzéteszi az összes kódolt szavazatot.
f) A szavazó elküldi a számlálónak a dekódoló függvényt. A számláló ennek alapján előállítja a szavazatot [sz].
g) Az ellenőr senki szavazatát nem láthatja, a számláló nem tudja, hogy melyik szavazat kihez tartozik.

Ez csak az alapötlet, használat előtt még finomítani kell (például ha így hagynánk, a szavazók be tudnák bizonyítani a választás után, hogy kire szavaztak). Bonyolultsága ellenére rendkívül gyors ez a protokoll, mert sok részlet automatizálható szoftverekkel.

Az 1990-es években Lorrie Faith Cranor és munkatársai a Washingtoni Egyetemről mások munkája nyomán kidolgozták a *Sensus* nevű protokollt.[7] Ez egy egyszerű, biztonságos és megfelelő adatvédelmet nyújtó protokoll az elektronikus szavazáshoz. Lényegében a borítékolt protokollt használja, kisebb módosítással.

Minden protokollnál feltételezni kell, hogy az ellenőr helyesen végzi a munkáját, azaz csak és kizárólag a szavazásra jogosultaknak engedélyezi a szavazást. A gyakorlatban ezeket a protokollokat érdemes hierarchikusan megvalósítani. Nagy számú szavazókör esetén célszerű, ha a szavazókörök mondjuk a megyei központba küldik el a szavazatokat, és ott számolják meg azokat. A megyei szintről ezek a kisebb központok az országos központba küldik el a saját eredményeiket, ahol a megyék eredményit összeadják. Ezzel a megoldással időt lehet spórolni, és kisebb teljesítményű gépek is elegendőek. Egy fontos dologra kell figyelni: minden szint csak az urnazárás után küldheti feljebb a saját eredményét. A választás végkimenetelét befolyásolhatja, ha megtudják a választók, hogy az egyik megyében melyik jelölt az abszolút esélyes.

2.1.5. Elektronikus szavazás a világban

Az Egyesült Államokban már a 2000. évi elnökválasztás kapcsán is sokat lehetett hallani az elektronikus szavazásról. Floridában lyukkártyás rendszert is használtak. Ezzel több probléma volt. Először is a szavazók közül sokan nem a pontos helyen lyukasztották ki a

[7] A Sensus-ról bővebben lásd: http://lorrie.cranor.org/voting/sensus/

kártyákat. Másodszor, nem tökéletesen lyukasztottak. Egy kis papírdarabka vagy ott maradt, vagy több vált le a kártyáról. Ezek miatt a számlálógép sokszor tévesen számolt. A külföldön tartózkodó katonák az interneten keresztül is szavazhattak. Ekkor két probléma lépett fel: inkompatibilitás a számítógépek és szavazóprogramok között, valamint a szerverek túlterheltsége.

A floridai kudarc után az összes állam úgy döntött, hogy felülvizsgálja saját elektronikus szavazórendszerét. Ennek ellenére a 2004-es választásokon az emberek 75 százaléka ugyanazokon a gépeken szavazhatott, mint 2000-ben. Nem így Nevada államban, ahol egy új rendszer bevezetése mellett döntöttek: a Sequoia Voting Systems érintőképernyős gépét használhatták a szavazók. Ezek a gépek papíron is dokumentálnak mindent, így ellenőrizhetőek az esetleges újraszámláláskor. A 2004. október 16-án kezdődött elnökválasztáson már ezt a rendszert használhatták az emberek. A rendszer fogadtatása pozitív volt. Elsősorban azért tetszett a szavazóknak, mert egyszerű a használata, így a szavazás menete is sokkal egyszerűbbé vált.

A 2004 novemberi választások után is több államban megkérdőjelezték a választások tisztaságát. Sokan úgy gondolják, hogy az elektronikus szavazórendszerek hibája miatt tudott George Bush újra nyerni. Ohio egyik szavazókörzetében például a feljegyzések szerint 638-an szavaztak. Ebből 260 szavazatot Kerry kapott, 4258-at pedig Bush. Ezek szerint Bush 3900 extra szavazatot kapott. Az ebben az államban használt gépek nem dokumentálták papíron a szavazatokat, ezért azok nem újraszámolhatóak. Nem lenne szabad olyan elektronikus rendszert használni, amely nem adja meg az újraszámolás lehetőségét, és amely fekete doboz, azaz pontos működését nem lehet ismerni. Ráadásul a hivatalnokok többsége nem ért a használatban lévő rendszerhez. Például nem tudták kinyomtatni és közzétenni az összes gép belső naplót tartalmazó fájljait.

A különböző hírműsorok és újságcikkek alapján furcsa kép rajzolódik ki. Az elektronikus szavazórendszert az emberek szívesen használják mindaddig, amíg nem derül ki az eredmény. Mivel a két jelölt között kevés volt a különbség, a vesztes fél támogatói megpróbáltak megtenni mindent annak érdekében, hogy mégis az ő jelöltjük nyerjen. A legegyszerűbb az volt, hogy az új, kevéssé ismert és sokak által nem elfogadott elektronikus szavazórendszerek korrekt működését vonják kétségbe.

Elektronikus szavazásra az Egyesült Államokon kívül is találunk példákat. 2001 áprilisában és májusában Svédországban a kaliforniai Safevote cég elektronikus választórendszerét használták. Az Umeai Egyetemen 12 500 diák szavazhatott egy őket érintő kérdésben az interneten keresztül, illetve személyesen. Mindenki annyiszor szavazhatott, ahányszor akart, ott, ahol akart és olyan módszerrel, amilyennel akart, de csak az utolsó érvényes

szavazatát vették figyelembe a szavazatszámlálásnál. Azonosításhoz elektronikus szavazói tanúsítványt (digital vote certificate — DVC) használtak, ami egy 6 karakter hosszú anonim kódolt elektronikus aláírásnak felelt meg. Ennek alapján mindenki ellenőrizhette, hogy a rendszer megkapta-e és elfogadta-e a szavazatát. Sajnos előfordulhatott, hogy valakinek a szavazata elveszett, de csak abban az esetben, ha a szavazóoldalon csalás történt.

Brazíliában és Hollandiában már használnak ATM-szerű szavazógépeket. Az eljárás hasonlít a hagyományos módszerre: a szavazópolgár egy meghatározott helyen adhatja le voksát, ott ugyanúgy egy fülkében választ a jelöltek közül, hiszen még mindig szüksége van arra, hogy nyugodtan, egyedül szavazzon. A szavazó egy speciális kártyát visz be magával, azt behelyezi a gépbe, melynek folyadékkristályos képernyőjére bökve kiválaszthatja a jelöltjét. A gép nemcsak a jelölt nevét és támogató pártját jeleníti meg, hanem egyéb információkat, mint például a programját, vagy akár a fényképét is. Ha egyszerre több mindenről kell dönteni a szavazáskor, akkor az egyik lista kitöltése után automatikusan megjelenik a következő. Ha a szavazó hibát vét, például két jelöltet jelöl be egy olyan listán, ahol csak egyet szabad, akkor a gép azt azonnal jelzi és a szavazónak azt ki kell javítania. Amikor elfogytak a listák, a gép még egyszer végigmegy rajtuk, és a szavazó megváltoztathatja döntését, ha véletlenül nem azt a jelöltet jelölte meg, amelyiket szerette volna. A szavazás végeztével a gépbe helyezett kártyát kell a szavazónak leadnia.

1997 őszén Costa Ricában a kormány felkérésére a Villanova University Law School tanárai és hallgatói az elektronikus szavazás kidolgozásán fáradoztak. A tervek szerint 2002-ben már lecserélték volna a papíralapú szavazást. Costa Ricában a szavazásra jogosultak csak ott szavazhatnak, ahol betöltötték a 18. életévüket. Éppen ezért a szavazás rendkívül költséges, a pártok buszokat fogadnak, benzinpénzt fizetnek szavazóiknak. Emiatt elég kevesen járulnak az urnákhoz. Mivel az iskolák nemzetközi támogatással számítógépparkkal és internetes kapcsolattal rendelkeznek, ésszerű megoldás lehet az elektronikus szavazás. A felkért szakértők több problémával találkoztak. Először is, a szavazók nagy része nem értett a számítógépek használatához. Másrészt, a vakok és gyengén látók képtelenek lettek volna a szavazásra, mivel nem látják a képernyőt; ezeket a számítógépeket látó gyerekek oktatására használják. Hiába az amerikai szakértők részvétele a programban, az USA politikája szerint kriptografikus szoftvereket nem lehet az államok területéről kivinni. Talán a legkomolyabb probléma a szavazók hozzáállása volt. Azok, akik nem értenek a számítógépekhez, és eddig sem vettek részt a választásokon, miért szavaznának most? 1998. elején a kormány leállította a programot.

2002-ben az Egyesült Királyságban elhatározták, hogy 2006-ban már az interneten keresztül fognak választani. Robin Cook, az alsóház vezetőjének a felügyelete alatt kezdődött meg a társadalmi vita. 2002 májusában öt választókörben helyi választásokat

tartottak, és Swindon szavazókörében az interneten keresztül is lehetett szavazni. Az eredmény: nem szavaztak többen, mint azt előre várták. Elektronikusan is inkább a férfiak, és a fiatalok szavaztak. A szavazófülkében voksoltak fele arra a kérdésre, hogy ők miért nem használták a számítógépeket, azt válaszolták, hogy ők inkább a megszokott, tradicionális módon kívánnak szavazni.

2004 őszén Svájcban két referendumon is lehetett elektronikus úton is szavazni. A választópolgárok kaptak egy kártyát, egy egyszeri használatra szóló személyi kódot és egy PIN-kódot, és ennek segítségével bármely internetre kapcsolt számítógépről leadhatták szavazatukat. Az elektronikusan szavazók aránya mindkét esetben meghaladta a 20 százalékot; technikai hibáról, panaszról nem érkezett bejelentés. Az évente átlagban legalább négyszer szavazó svájci polgárok 2005-ben már Genfben és Zürichben is kipróbálhatják az új rendszert.

2.1.6. Érvek — ellenérvek

A politikusok az elektronikus szavazástól azt várják, hogy olcsóbb lesz a szavazás, és hogy azok is szavazni fognak, akik eddig ezt nem tették. 2002 júliusában a BBC egy nemzetközi közvélemény-kutatást rendezett az elektronikus szavazással kapcsolatban. Az eredmény nem nyugtatta meg a politikusokat, a válaszadók többsége ellenezte az elektronikus szavazást.

Az elektronikus szavazást támogató állampolgárok fő érvei:

- egyszerűbben, gyorsabban lehetne majd szavazni;
- a vakok, gyengén látók és mozgássérültek is könnyebben szavazhatnak majd;
- kevesebb pénzzel megoldható a szavazás.

Az ellenzők többen vannak. Érveik:

- biztonság — félnek, hogy az interneten keresztüli szavazásnál nem lehet megfelelő szintű biztonságot elérni;
- az emberek nagy része nem ért a számítógépekhez, nem bízik meg bennük. Még azok sem, akik irodában, gépekkel dolgoznak, hiszen ők látják, hogy a gépek elromlanak, lefagynak stb.;
- tradíció, azaz a szavazásnak van egyfajta ceremoniális hangulata, amit nem szabad elveszíteni.

Természetesen az lenne a legjobb, ha választani lehetne a hagyományos és az elektronikus szavazás közül. Az elektronikus szavazás legfőbb érve, és amiért igazán érdemes lenne bevezetni, az a mozgásukban korlátozott emberek segítése. Minden állampolgárnak egyenlő esélyeket kell teremteni a szavazáskor is. Ezt kell figyelembe venni elsősorban, és nem azt, hogy hányan értenek a számítógépekhez.

Társadalomkutatók elemzése szerint a ma nem szavazók, politikával nem foglalkozók nagy része nem a papír alapú szavazás miatt nem szavaz. Ők kiábrándultak a politikából és a politikusokból, akik nem teljesítik választási ígéreteiket. Ennek köszönhető például, hogy a Big Brother show szereplőire szinte minden európai országban sokkal többen szavaznak, mint amennyien az urnákhoz járulnak négy-öt évente.

3. A bioszkript

A bioszkript az angol biometric encryption (biometrikus rejtjelezés) szavak összevonásából jött létre, kifejlesztője és szabadalmaztatója a kanadai Mytec (ma már Bioscrypt) cég. A bioszkript az úgynevezett PET technológiák (Privacy Enhancing Technologies, „magánélet-növelő technológiák") körébe tartozik, amelyeket az adatalanyok védelme érdekében fejlesztettek ki.[8]

A bioszkript, mint elnevezéséből is kitűnik, biometriát alkalmaz a technológia alapelemeként. Ahhoz, hogy a bioszkript alkalmazásának előnyös lehetőségeit megértsük, tekintsük át a biometrikus rendszerek működésének néhány általános jellemzőjét.

3.1. Hogyan működnek a biometrikus rendszerek?

Mielőtt valakit biometrikusan azonosítani akarunk, mintát kell vennünk. Ezt a mintát, maszkot fogja a jövőben használni a rendszer. Regisztráláskor általában nem csak egy mintát vesznek, hanem többet, és átlagolják ezeket. Ez a folyamat kritikus, mert egy rossz maszk félreértéseket, hibás azonosítást eredményezhet.

A maszkot három helyen lehet tárolni: a biometriai olvasóeszközön, egy központi adatbázisban és egy adathordozón. Ha az olvasóeszközön tároljuk a maszkot, akkor gyors felismerést vagy elutasítást tehetünk lehetővé, ha csak egy olvasóeszközünk van. Azonban az eszköz sérülése esetén akár az összes maszk megsemmisülhet. Egy központi adatbázisban tárolt maszkok előnye, hogy nincs korlátozva a maszkok száma, mérete, és egy olvasó eszköz kiesése esetén nem semmisülnek meg a maszkok. Hátránya viszont,

[8] Bővebben lásd Székely I.: PET technológiák: a személyes adatok védelmének korszerű eszközei.

hogy megbízható és gyors hálózat kell, melynek meghibásodása az egész azonosító rendszert alkalmazhatatlanná teszi. Megfelelő algoritmus kell továbbá a nagy adatbázisban való kereséshez. Ha egy adathordozón, például kártyán tároljuk a maszkot, akkor nem kell foglalkozni adatbázisokkal, és bármelyik olvasóeszközt használhatja a felhasználó. Ügyelni kell viszont a kártya sértetlenségére. Komolyabb probléma, hogy egységes olvasó eszközök szükségesek ehhez a megoldáshoz. A legjobb megoldás, ha egy adathordozón és egy központi adatbázisban is tároljuk a maszkokat.

Ellenőrzéskor a felhasználó megadja PIN kódját, vagy megmutatja azonosító kártyáját, hogy igazolja magát. Majd ezt megerősíti egy biometriai adattal is, amelyet összehasonlítanak a referenciamaszkkal. Az eredmény pozitív, vagy negatív. Megjegyzendő, hogy bizonyos időközönként a maszkot frissíteni kell. Néhány rendszer ezt megteszi automatikusan, a felhasználó minden belépésekor.

Előfordul, hogy a rendszer, ha elutasító választ ad, azt kommentálja is. Vagyis megmondja, hogy a vizsgált biometrikus kép mennyire hasonlít a maszkhoz. Ez veszélyes, mert ha valaki hozzájut egy maszkot tartalmazó kártyához, azt használni is tudja. Egyszerűen készít egy képet, megmutatja az olvasó eszköznek, ami megmondja, hogy ez a kép mennyire hasonlít a maszkhoz. Ezután már nincs más dolga szélhámosunknak, mint addig-addig változtatni a képét, amíg a rendszer végül el nem fogadja. Ezt a támadási formát az angol nyelvű szakirodalom hill-climbing attack néven ismeri.[9]

3.2. Kulcsok, jelszók biometrikus tárolása

A biometriát sokféleképpen lehet felhasználni kulcs, jelszó stb. biztonságos tárolásához.[10] Az egyik megoldásban a kulcsokat, jelszókat egy biztonságos helyen tárolják. A felhasználó reprodukálja a biometrikus adatot, azt a rendszer ellenőrzi. Ha sikerült a felhasználót azonosítani, akkor a biztonságos helyen tárolt jelszó bekerül a rendszerbe és a felhasználó hozzájuthat, amihez szeretne. Vagyis a megoldás lényege, hogy a felhasználónak nem kell megjegyeznie a jelszavát, hanem azt a biometrikus adat alapján nyerik ki.

A második lehetőség, hogy a kulcsot elrejtik egy titkos bitcserélő algoritmussal a felhasználónak a rendszerben tárolt ujjlenyomatának képében. Ha a felhasználót azonosította a rendszer, akkor kinyerik az elrejtett kulcsot. Ennek a megoldásnak a

[9] Erről bővebben lásd Colin Soutar Biomeetric System Security című írását (www.bioscrypt.com).

[10] E fejezet írásakor Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, és B.V.K. Vijaya Kumar Biometric Encryption™ című munkájára támaszkodtunk.

hátránya, hogy minden felhasználónál a kulcsot ugyanarról a helyről nyerik és, ha a támadó megfigyeli, hogy melyik helyekről nyerik ki a kulcsot, akkor elő is tudja majd állítani.

A harmadik esetben magából a biometrikus adatból, a reprodukált ujjlenyomatból nyerik ki a kulcsot. Ennek két hátránya van. Egyik, hogy a biometrikus adatot nem lehet úgy reprodukálni, hogy az tökéletesen olyan legyen, mint az előző, vagyis nem biztos, hogy a kulcs minden esetben ugyanaz lesz. Másik hátránya pedig, hogy ha a támadó egyszer hozzájut a kulcshoz, akkor ő is be fog tudni lépni a rendszerbe. Ezt csak úgy lehetne kiküszöbölni, ha cserélik a jelszót, vagyis cserélni kell a biometrikus adatot, ami nem mindig lehetséges (ujjlenyomatot meg lehet változatni, de a retinát nem).

3.3. A bioszkript koncepciója

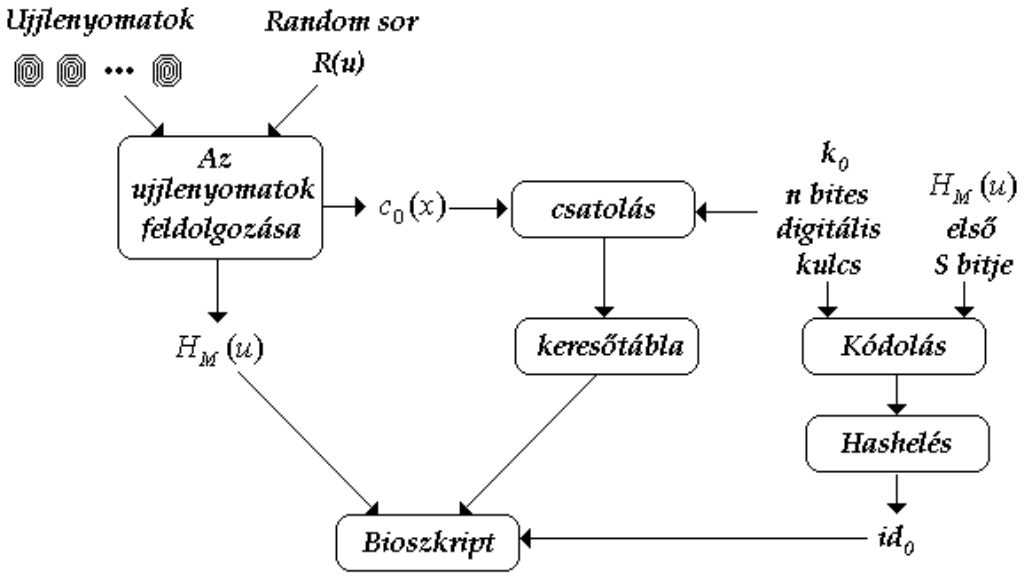
A bioszkript egy negyedik megoldást kínál. Nem külön történik a felhasználó azonosítása és a kulcs eleresztése, hanem a kulcsot még a felhasználó felvételekor csatolják a biometrikus adathoz, és később az azonosításkor ki is nyerik azt. A bioszkript mindig két alapelemből áll: egy biometrikus és egy nem biometrikus elemből. Az előbbi a megvalósított rendszerben egy digitalizált ujjlenyomat, de ujj helyett felhasználható a fül, a hang vagy más biometrikus adat. A nem biometrikus elem lehet például PIN kód, pointer, kulcs. A bioszkript egyik tulajdonsága, hogy nem lehet kinyerni belőle sem a biometrikus, sem a nem biometrikus adatot egymástól függetlenül, és az sem tudható, hogy kinek az ujjlenyomatát használták fel a létrehozásához. Ha a tulajdonos reprodukálja az ujjlenyomatát, azzal felszabadítja a nem biometrikus adatot, aminek segítségével hozzájuthat a védett adatokhoz vagy beléphet a rendszerbe. Másik tulajdonsága, hogy a nem biometrikus adat, egy digitális kulcs, teljesen független az ujjlenyomattól, így azt később cserélni, módosítani lehet. Ha a kulcs használhatatlanná válik, a biometrikus adat attól még használható, nem kell kidobni.

A megoldás három alapvető elvárást teljesít:

1. Sem a felhasználó ujjlenyomata, sem a kulcs nem nyerhető ki belőle.
2. Rugalmasan viselkedik az ujjlenyomatok torzulására. Ez azt jelenti, hogy képes felismerni a reprodukált ujjlenyomatot akkor is, ha a felhasználó ferdén rakta rá a leolvasóra, vagy nedvesebb a keze.
3. Felismeri az összes felhasználót, illetve ha egy támadó ujjlenyomatát kapja, akkor egy illegális kulcsot produkál (vagyis a támadó nem tud hozzáférni a védett adatokhoz, rendszerhez).

A bioszkript létrehozásának részletes algoritmusát e tanulmány Függelékében ismertetjük. Az alábbiakban a bioszkript előállításának és használatainak főbb lépéseit mutatjuk be.

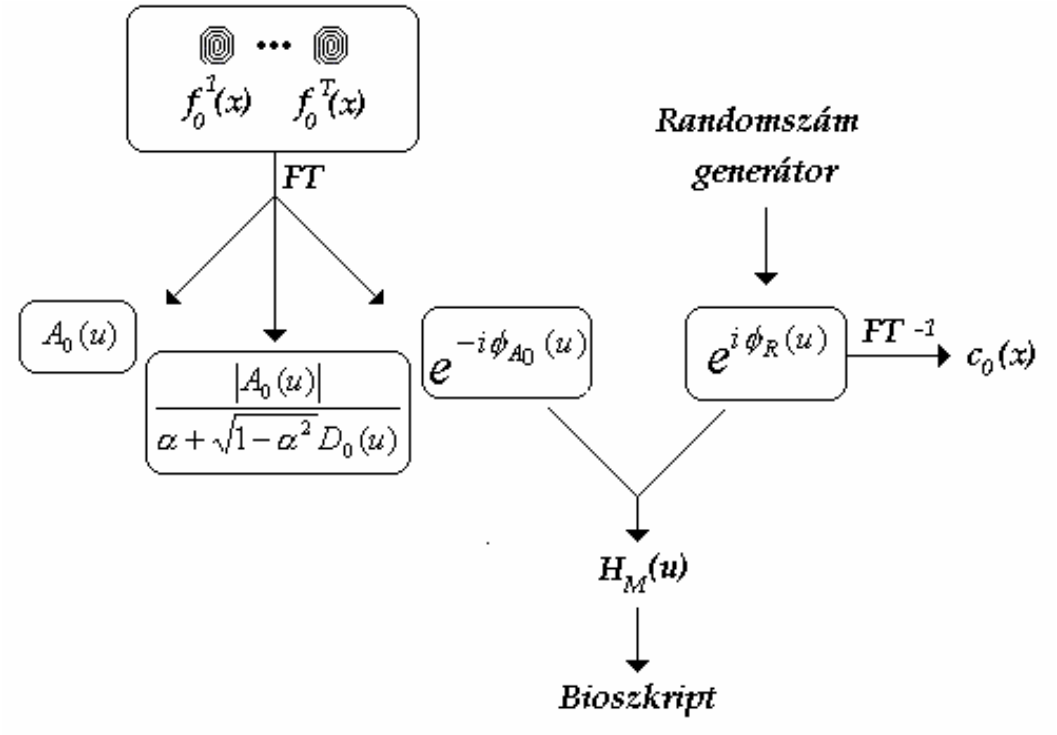
3.4. A bioszkript előállítása



1. ábra: A bioszkript előállítása

A bioszkript előállításához szükség van egy nem biometrikus adatnak az ujjlenyomathoz való hozzáfűzésére. A nem biometrikus adat egy n bites digitális kulcs, k_0, ami lehet véletlenszám-generátor által generált, vagy kívülről kapja a bioszkriptet előállító algoritmus. A bioszkript előállításához tehát végül is három elemre van szükség: T darab ujjlenyomatra, a véletlenszám-generátorral generált R(u)-ra, és k_0-ra.

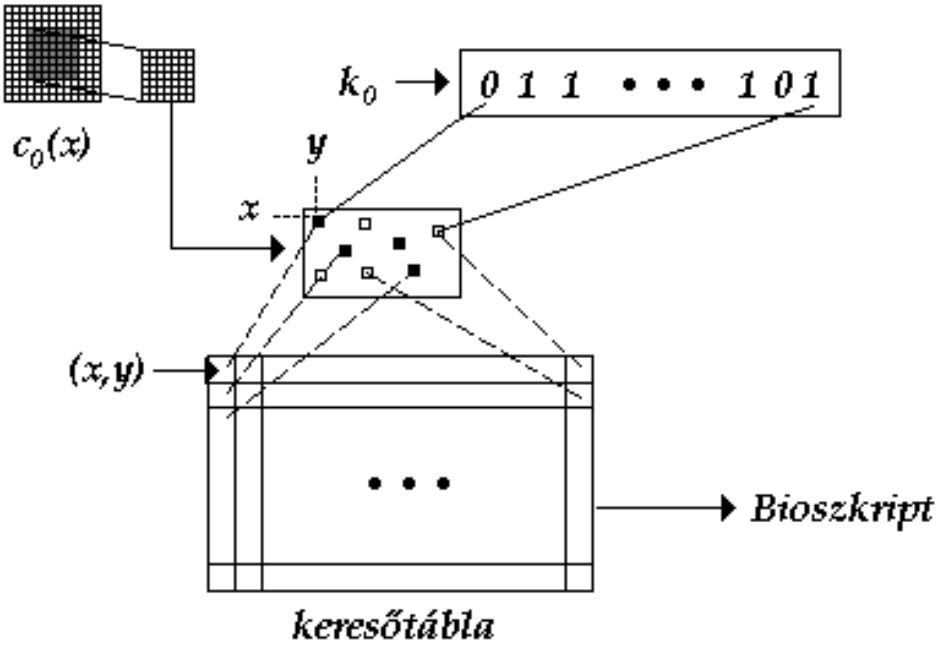
3.4.1. Az ujjlenyomatok felvétele és feldolgozása



2. ábra: Az ujjlenyomatok feldolgozása a bioszkript előállításakor

A T számú (általában 4 vagy 6) ujjlenyomatot felhasználva előállítják a H(u)-hoz szükséges $D_0(u)$-t, $A_0(u)$-t és annak egyéb formáit. A random R(u) és $A_0(u)$ fázisának komplex konjugáltjából előállítják $H_M(u)$-t, amit tovább felhasználnak majd a bioszkript előállításához. R(u) segítségével előállítják $c_0(x)$-et (egy 128×128-as tömb komplex értékekkel), amit továbbadnak a csatoláshoz.

3.4.2. Csatolás



3. ábra: A csatolás menete

Ilyenkor csatolják $c_0(x)$-hez az n bites k_0 kulcsot, amivel a felhasználó be tud jutni a rendszerbe. Az eljárás alatt egy keresőtáblát hoznak létre, amit tárolnak is a bioszkriptben, hogy felhasználhassák, amikor a felhasználó azonosítani szeretné magát. Mivel a bioszkript előállításakor felhasznált ujjlenyomatok nem tökéletesen ugyanolyanok, mint azok, amelyeket a felhasználó azonosításkor reprodukál, ezért a belőlük nyert kimenet sem lesz egyforma. Az azonosításkor kapott kimenet legyen $c_1(x)$. Sokféle lehetőség van a csatolásra, ezek közül is több használ hibajavító kódolást. Az egyik lehetséges megoldás ismétlődő kódolást alkalmaz, $c_0(x)$-nak csak a központi 64×64-es részét használja. Azért van szükség erre a kivonatra, hogy az azonosításnál is ugyanazt az eredményt kapják. Ebből a 64×64-es részből nyerik ki az összehasonlításhoz használt mintát, ami 128 sorból és 64 oszlopból áll. Ezt úgy kapják, hogy szétválasztják $c_0(x)$ elemeinek valós és képzetes részeit. Ha (x,y) helyen $\boldsymbol{a}+\boldsymbol{bi}$ elem áll, akkor $\boldsymbol{a}$ a mintában az (x,y) helyen fog szerepelni, míg $\boldsymbol{b}$ az (x+64,y) helyen. A mintatábla így 8192 valós értéket tartalmaz, jelöljük őket d-vel. Minden elemet binárissá változtatnak a következő módon:

$$d \to 1, \text{ ha } d \geq 0.0$$

$$d \to 0, \text{ ha } d < 0.0$$

Tegyük fel, hogy k_0 első bitje 0. Ekkor L olyan koordinátát választanak a mintatáblából, ahol az elem értéke 0. Ezt az L pozíciót tárolják el a keresőtábla első oszlopában. Ezt az

eljárást folytatják, amíg el nem jutnak k_0 végére. A mintatábla minden eleme k_0-nak csak egy bitjét reprezentálhatja. Így jutnak el a 128 oszlopot tartalmazó keresőtáblához, amelynek minden oszlopa L pozíciót tartalmaz. L megválasztásához a következőket veszik figyelembe:

1. L-nek 1-nél nagyobbnak kell lennie, hogy biztosítsa a redundanciát a kulcs későbbi kinyerésénél.
2. L ne lehet akármilyen nagy, hogy szélsőséges esetekben is legyen megfelelő mennyiségű elem a mintatáblában. Pl. ha k_0 nagyon sok 0-t tartalmaz, akkor kell találni annyiszor L db 0 elemet a táblában, ahány 0 van k_0–ban.
3. Ügyelni kell, hogy az L elem minden bitre úgy legyen kiválasztva, hogy a keletkező hibavalószínűség minél kisebb legyen minden egyes bitre.
4. L legyen páratlan, hogy alkalmazható legyen a többségi döntés.

3.4.3. Azonosító kód előállítása

Szükség van egy olyan eljárásra, ami ellenőrzi, hogy a kinyert kulcs valódi kulcs-e. Hiszen ha egy támadó be szeretne jutni a rendszerbe, akkor egy illegális k_0 kulcsot állít elő azonosításkor, és a rendszer feleslegesen próbálkozik a dekódolással. Viszont nem célszerű magát k_0-át tárolni a bioszkriptben, helyette kódolással és hash-eléssel előállítják id_0-t, egy azonosító kódot. Az azonosításkor nyert k_1-ből ugyanezzel az eljárással szintén előállítanak egy azonosítót, id_1-t, és ezeket összehasonlítva döntik el, hogy a kinyert kulcs valóban valódi-e.

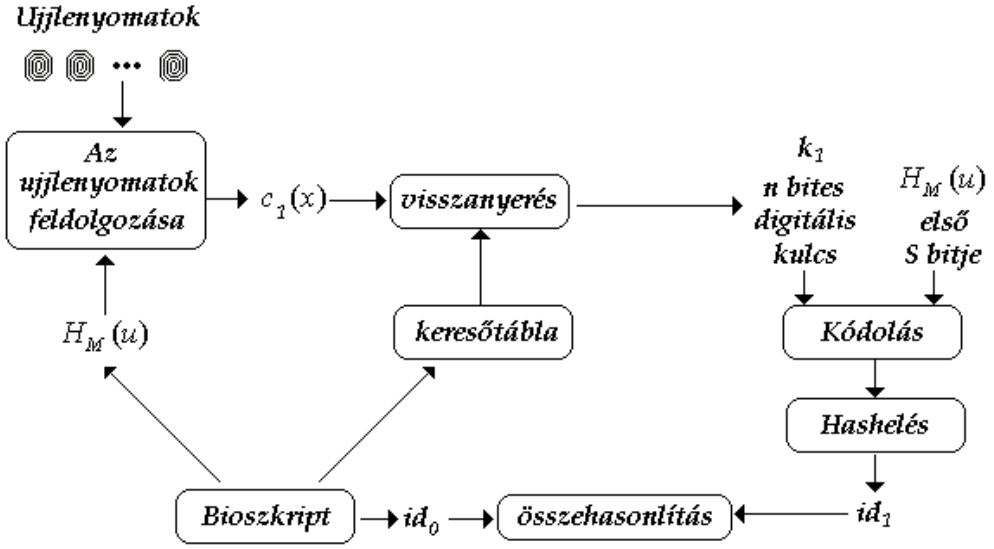
Először k_0 kulccsal kódolnak S bitnyi információt, majd a kódolt adatot egyirányú hash függvénnyel hashelik. Az így kapott azonosító kódot tárolják a bioszkriptben. Az S bitnyi információ célszerűen olyan, ami elérhető mind a felhasználó felvételekor, mind az azonosításakor. Ezen kívül fontos még, hogy ez az információ minden felhasználónál más legyen. Mivel $H_M(u)$ mindkét feltételt kielégíti, ezért $H_M(u)$ első S bitjét használják fel ehhez. A kódoló algoritmus és a hash függvény megválasztása független a bioszkripttől, csak biztonságosnak kell lenniük. (A kódoló algoritmusra jó példa a 3DES,[11] a hash függvényre pedig az SHA-1.[12])

Ezután már csak rögzítik $H_M(u)$-t, id_0-t és a keresőtáblát valamilyen arra alkalmas tárolóeszközre, és így előállt a bioszkript.

[11] A 3DES-ről bővebben lásd: http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html

[12] Az SHA-1 algoritmusról bővebben lásd: http://www.itl.nist.gov/fipspubs/fip180-1.htm

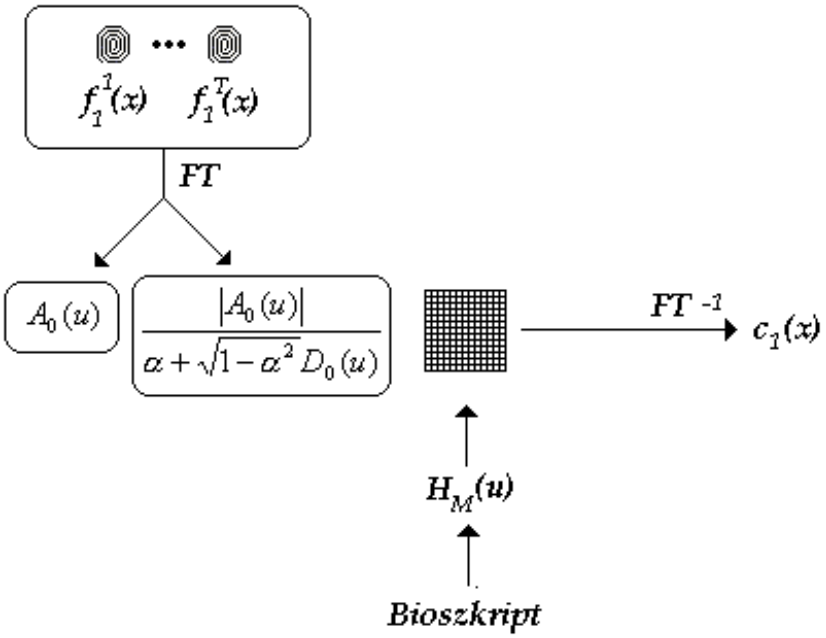
3.4.4. Verifikálás



4. ábra: A verifikálás folyamata

A verifikálás célja, hogy a legális felhasználónak előállítsa az n bites kulcsot, k_0-át, a támadót pedig ne engedje be a rendszerbe.

3.4.5. Az ujjlenyomatok feldolgozása verifikálásnál

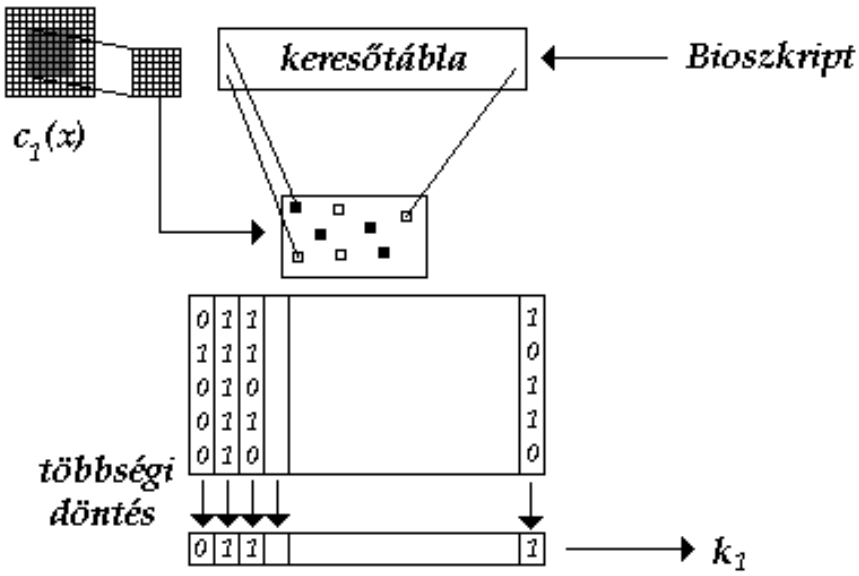


5. ábra: Az ujjlenyomatok feldolgozása verifikálásnál

Verifikálásnál is T darab ujjlenyomatra van szüksége a rendszernek $A_1(u)$ és $D_1(u)$ előállításához. A bioszkriptből nyert $H_M(u)$ segítségével előállítják $c_1(x)$-et, amit tovább az n bites kulcs előállításához használnak.

A rendszer biztonságára vonatkozó megfontolásokat ugyancsak a Függelékben ismertetjük.

3.4.6. A kulcs kinyerése



6. ábra: A kulcs kinyerése a bioszkriptből

3.4.7. A kinyerési algoritmus lépései

1. $c_1(x)$ központi 64×64-es részének kinyerése.
2. A csatolásnál megismert módon szétválasztják a valós és képzetes részeket, hogy csak egy 128×64-es valós értékeket tartalmazó tábla maradjon, és az ott megismert módszerrel binárissá változtatják az értékeket. Így kapják meg a mintának használt táblázatot.
3. A keresőtáblát felhasználva, többségi döntéssel meghatározzák k_1-et. A kulcs n. elemét úgy kapják, hogy összeadják azokat az elemeket, amelyeknek a pozíciója a keresőtábla n. oszlopában van meghatározva. Ha az összeg nagyobb, mint L/2, akkor az n. bit 1, egyébként pedig 0 (többségi döntés).
4. A kulcs érvényességének ellenőrzése.
5. Ha a kulcs legális, akkor kiengedik a rendszerbe. Ha nem legális, akkor visszatérnek $c_1(x)$-hez és azt a 64×64-es részt használják fel, aminek a központja

egy pixelnyi távolságra van $c_1(x)$ központjától. Ismétlik az eljárás lépéseit 2-től 5-ig, úgy, hogy felhasználják az összes olyan részt, aminek a központja $c_1(x)$-től egy pixelnyire van, két pixelnyire van, három pixelnyire van stb., körülbelül 16 pixelnyi távolságig. Ha közben valamelyik kulcs jónak bizonyult, akkor azt kiengedik a rendszerbe. Ha egyik kulcs sem legális, akkor egy „sikertelen azonosítás" üzenetet küld a rendszer.

Tapasztalatok szerint a ±16 pixelnyi eltolás elegendő egy valódi felhasználó felismeréséhez, és nem túl sok ahhoz, hogy egy támadót beengedjen a rendszer.

3.4.8. A kulcs érvényességének ellenőrzése

Ahhoz, hogy megtudjuk, k_1 érvényes-e, meg kell tudnunk, hogy azonos-e k_0-val. Ehhez ki kell számolnunk id_1-t, amit összehasonlítunk a bioszkriptben eltárolt id_0-val. Az azonosító kód, id_1 előállítása ugyanúgy történik, mint ahogy id_0-é történt. Tehát k_1-et kulcsként használva kódolják $H_M(u)$ ugyanazon S bitjét, majd a kódolt adatot hash-elik, így kapva id_1-t. Ezután összehasonlítják a két azonosító kódot. Ha $id_1 = id_0$, akkor a k_1 nagy valószínűséggel megegyezik k_0-val, és a kulcsot kiengedhetik a rendszerbe. Egyébként k_1 nagy valószínűséggel nem egyezik meg k_0-val és a kulcs kinyerési algoritmust folytatni kell, vagy „sikertelen azonosítás" üzenetet kell küldeni.

3.5. A rendszer működésének összefoglalása

- Minden felhasználótól T darab (általában T=4 vagy 6) ujjlenyomatot vesznek.
- Minden felhasználónak generálnak egy R(u) függvényt, és k_0 kulcsot (ez esetleg lehet kívülről kapott is).
- Az ujjlenyomatokat és R(u)-t feldolgozva megkapják $H_M(u)$-t (a szűrésre használt függvény), illetve $c_0(x)$-et (egy 128×128-as tömb, a rendszer válasza az ujjlenyomatokra).
- k_0-t és $c_0(x)$-et felhasználva előállítják a keresőtáblát (csatolják k_0-t $c_0(x)$-hez)
- k_0-t kulcsként használva kódolják $H_M(u)$ első S bitjét, az eredmény hash-elésével előállítják id_0-t.
- $H_M(u)$-t, a keresőtáblát és id_0-t tárolják a bioszkriptben (a tároló eszköz szinte bármi lehet).
- A felhasználó reprodukálja az ujjlenyomatát.
- A bioszkriptben tárolt $H_M(u)$ és az ujjlenyomat alapján előállítják $c_1(x)$-et.
- A bioszkriptben tárolt keresőtábla és $c_1(x)$ alapján előállítják k_1-et.
- $H_M(u)$ első S bitjét k_1 kulccsal kódolják, majd hash-elik, az eredmény id_1.

- Összehasonlítják id_1-t és id_0-t. Ha ezek egyformák, akkor a felhasználó legális és be lehet engedni a rendszerbe, ha nem, akkor egy támadó próbált bejutni és ezt elutasítják.

A biometrikus rejtjelezést alapvetően ujjlenyomat felhasználására fejlesztették ki, de kis változtatással használható egyéb biometrikus adattal is. A lényeg, hogy a biometrikus adatot olyan képpé kell transzformálni, aminek olyan tulajdonságai vannak, mint az ujjlenyomat képének (nagyság, felbontás stb.). Például ha a retina képét használják fel, akkor az algoritmus egyszerűsödik egy kicsit, hiszen a pupilla felhasználható referenciapontnak, így a rejtjelezésnek nem kell transzformáció-invariánsnak lenni, tehát Fourier-transzformáció helyett felhasználható egyéb transzformáció is (pl. Gabor transzformáció). Ezenkívül a deformáció és egyéb változások sem olyan nagy mértékűek, mint az ujjlenyomatnál, így nem is kell annyira toleránsnak lennie, ebből következően biztonságosabb is lesz a rendszer.

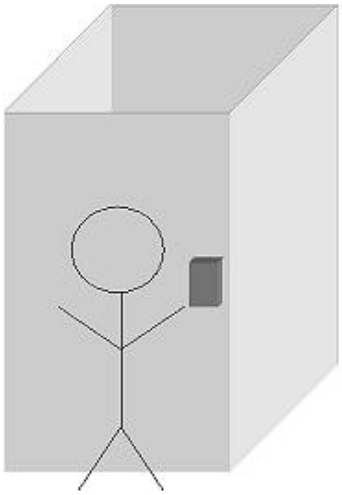
4. A bioszkript az elektronikus szavazásban

Állításunk szerint a bioszkript alkalmazása az elektronikus szavazásban minden, a szavazással szemben támasztott követelménynek megfelel. Két általunk elképzelt rendszert mutatunk be és elemzünk, és végül kitérünk a bioszkript használatának előnyeire is.

Mindkét elképzelés hasonló a mai szavazáshoz abból a szempontból, hogy a szavazás szavazóhelyiségben történik. A nem szavazóhelyiségből történő elektronikus (otthonról, munkahelyről, kávézóból stb. interneten, telefonon, kábeltévén stb. keresztül) szavazással kapcsolatban csak a megoldandó problémákra térünk ki. Mindkét rendszer használhat egy intelligens kártyát, amely a szavazásra jogosult állampolgárok ujjlenyomatából előállított bioszkriptet tartalmazza. A bioszkript létrehozásával, a kártya elkészítésével, milyenségével, szétosztásával most nem foglalkozunk.

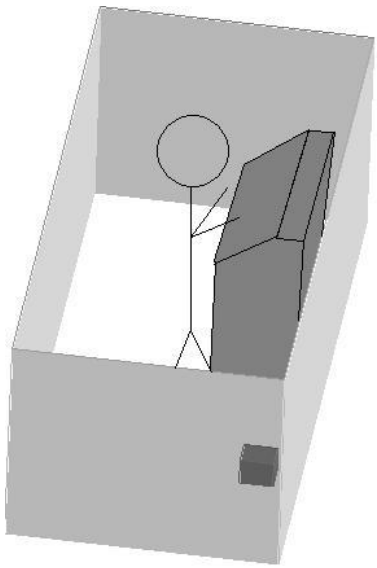
4.1. Az első rendszer

Az első megoldásban a választópolgár azonosítása és a szavazás egymástól élesen elkülönül. A szavazás érintőképernyős automatákon zajlana. A szavazógép egy ugyanolyan fülkében lenne elhelyezve, mint amilyenben a papír alapú szavazáskor a szavazólapokat kitöltjük. A fülkébe csak a szavazásra jogosultak juthatnak be bioszkriptjük, illetve az abból ujjlenyomatukkal kinyert kulcs segítségével. A fülke bejáratánál reprodukálniuk kell az ujjlenyomatukat, és ha a rendszer felismeri a felhasználót, aki jogosult a szavazásra és még nem szavazott, akkor a belépés szabad lesz. Vagyis a fülke ajtaja csak akkor nincsen zárva, ha olyan szavazópolgár szeretne bejutni, aki még nem szavazott, illetve szavazás után



7. ábra: Bioszkriptet használó fülke bejárata

szabadon ki lehet jönni. A kapu össze van kötve a szavazógéppel. A kapu jelzést küld, ha egy szavazó belép a fülkébe, illetve a gép jelez, ha a választópolgár szavazatát sikeresen eltárolták. Amikor a fülke üres, akkor a gép egy előre meghatározott képet jelenít meg. Ez lehet reklám, egy sima kép vagy valamilyen a szavazásra vonatkozó információ, mint például mikor, hol és meddig lehet az eredményeket megtekinteni. Amint egy szavazó belép a fülkébe, vagyis a kapu jelzi a gépnek, hogy legális felhasználó lépett be, a gép megjeleníti a szavazólapot. Ezek után a szavazás az előző fejezetekben leírtak szerint fog történni: a szavazó kiválasztja a jelöltjét, esetleg jelöltjeit a szavazólapon, amin nemcsak a jelölt neve jelenik meg, hanem akár fényképe és programja is. Ha van további kitöltendő lap, akkor a következőt jeleníti meg a gép. A gép jelez, ha a szavazó hibát vét (például több jelöltet jelölt be, mint amennyi a megengedett), s ezt ki kell javítania. Az összes lap kitöltése után a szavazó végignézheti választását, és változtathat rajta. Amikor a szavazó véglegesíti szavazatát, kap egy bizonylatot, hogy a szavazatát sikeresen eltárolták, s ekkor jelez vissza a gép a kapunak, hogy a szavazó már szavazott, többé nem engedheti a rendszerbe. Ezután a gép az előre meghatározott képet jeleníti meg ismét, egészen addig, amíg egy új felhasználó nem jön szavazni. Ez azt is jelenti, hogy ha valaki átmászik a kapun, vagy valamilyen más módszerrel bejut a fülkébe, akkor sem fog tudni szavazni, hiszen nem fog szavazólapot látni. Az azonosítás és a szavazás teljesen szétválik, és mivel a kapu nem tárolja, hogy ki mikor lépett be (sőt eleve nem ismeri a bioszkript kiinduló ujjlenyomatát, illetve az ahhoz tartozó személyt), ezért nem lehetséges összekötni az egyes szavazókat és szavazataikat.



8. ábra: Azonosítás után szavazógép segítségével lehet voksolni

Ebben a megoldásban a bioszkriptek a kapu rendszerében vannak tárolva, ezért ennek sérülése gondot okozhat, de erre van megoldás. Feltételezhetjük, hogy nem egy olyan fülke van, ahol bioszkript segítségével azonosítják magukat a szavazók (természetesen, ha csak egy kapunk van, akkor is használható lesz a megoldás). Így felmerül még egy probléma, nevezetesen a konzisztencia, vagyis hogy minden kapu adatbázisa mindig ugyanazt tartalmazza, mint a

többi. Ez azt jelenti, hogy ha a szavazópolgár szavazott már (akár elektronikusan, akár a hagyományos módszerrel), akkor már egyik kapun se juthasson be. A megoldás az, hogy nem a kapukban tároljuk a bioszkripteket, hanem egy központi nyilvántartásban, amivel az összes kapu kapcsolatban van. Így tehát, ha valaki elektronikusan szavazott, az azonnal megjelenik az adatbázisban. Ha pedig valaki papír alapon szavazott, akkor a bizottságnak kell manuálisan bevinnie a változást. Ehhez egy egyszerű terminálra lesz szükség, ahonnan ki lehet keresni az illetőt valamilyen azonosító szerint (név + anyja neve vagy a személyi igazolvány száma) és rögzíteni a szavazás tényét. A szavazótól továbbra sem kérhetnek el több adatot, mint amennyi az azonosításához szükséges és elégséges.

Van egy tartalék központunk, ez forró tartalék, ami azt jelenti, hogy a másik sérülése esetén ez azonnal át tudja venni a szerepét. Természetesen a központi adatbázist, az adatbázist és a kapukat összekötő kábeleket, illetve a kapukat a szavazógépekkel összekötő kábeleket megfelelően védeni kell.

Egy másik megoldás erre a problémakörre, hogy a bioszkripteket nem egy adatbázisban tároljuk, hanem egy intelligens kártyán, amit a kapuban elhelyezett nyílásba kell behelyezni és egészen addig ott is marad, amíg a szavazó ki nem jön a fülkéből, hiszen rögzíteni kell rajta a szavazás megtörténtét. Ezt persze úgy kell elképzelni, mint a készpénz-automatákat, vagyis a kártya nem lóg ki, senki sem tudja kivenni, miközben a tulajdonosa szavaz. Ennél a megoldásnál már csak azzal kell foglalkozni, hogy aki papír alapon szavaz és van intelligens kártyája, annak a kártyáján szintén megjelenjen, hogy már szavazott. Ennél a megoldásnál külön meg kell említenünk egy problémát, amit később általánosságban is kifejtünk: mi történik, ha a gép meghibásodik szavazás közben. A szavazó szavazatát nem számolja a rendszer, hiszen nem tudta elmenteni, vagy lehet, hogy még nem is sikerült véglegesítenie azt. Viszont a szavazó az intelligens kártyáját sem kapja vissza, hiszen a kapu nem kapott jelzést, hogy a szavazatot sikeresen eltárolták. A leggyorsabb megoldás, hogy az illető papír alapon szavaz, a meghibásodott fülkét lezárják, az intelligens kártyát az állampolgár később visszakapja. Egy elegánsabb megoldás, ha egy erre a célra kifejlesztett eljárással (például speciális bemenet használata) az intelligens kártyát visszanyerik, ellenőrzik a rajta tárolt adatok sértetlenségét és az esetleges hibákat javítják, majd visszaadják a tulajdonosnak, aki újra voksolhat egy másik fülkében. A meghibásodott gépet cserélhetik; ha lehetséges, megjavíthatják, vagy egyszerűen csak lezárják a fülkét. Természetesen a hiba megtörténtét rögzíteni kell a megfelelő módon és helyen.

4.2. A második rendszer

A második rendszer koncepciója hasonló az előbbihez; itt csak a leglényegesebb sajátosságait említjük. A fülkében egy számítógép található, mellette egy ujjlenyomat-leolvasó, kártyaleolvasóval együtt. Miután a szavazó azonosította magát a kártyája, a kártyán tárolt bioszkriptje és az ujjlenyomata alapján, a leolvasó készülék jelzi a számítógépnek, hogy egy szavazásra jogosult személy van a fülkében. A szavazó azonosítóját, bármilyen adatát a számítógép nem tudhatja meg. A gép ekkor engedélyezi egy szavazat leadását. Ez történhet billentyűzet, vagy érintésre érzékeny monitor segítségével.

Az azonosítást a rendszer kétszer is kérheti egymás után, ez még biztosabb azonosítást jelent. A rendszer lehetővé teszi, hogy a szavazat leadása előtt a képernyőn a szavazással kapcsolatos információk jelenjenek meg, sőt az is lehetséges, hogy a rendszer kép- és hanganyagot tároljon a jelöltekről. A hanganyag meghallgatásához fülhallgatót ajánlunk, így a fülkéből egyetlen jelölt kampánybeszéde sem hallatszik majd ki. Szavazás után a választópolgár elhagyja a fülkét, a kártyájával együtt.

A fülkében elég nagy értékű rendszer van. Ezért, és azért, hogy a szavazó csak rendeltetésszerűen használhassa a számítógépet, természetes igény a fülke megfigyelése. Akárcsak a bankautomatáknál, a fülkében is elhelyezhető egy kamera vagy fényképezőgép a számítógép mellett. Fontos, hogy a fényképeken, illetve a kamerákon nem látszódhat sem a monitor, sem a billentyűzet. Még a biztonsági személyzet sem tudhatja, hogy ki kire szavazott!

4.3. A rendszerek felépítése

4.3.1. Szavazat-feldolgozás

Mindkét rendszert hierarchikusan képzeljük el. A hierarchiaszintek száma a szavazókörök számától függ, erre most nem térünk ki. A fülkében lévő számítógép feletti szinten egy adatbázis található. Rekordjai a szavazatok. Esetleg az is szerepelhet az adatbázisban, hogy melyik szavazatot melyik gépnél adták le.

A két rendszer a szavazatokat többféleképp kezelheti. Az egyik megoldás állandó összeköttetést feltételez a magasabb hierarchiaszinttel, a másik szerint a szavazógép csak időnként kapcsolódik hozzá, és egy harmadik szerint egyáltalán nincs összeköttetés. Ha az összeköttetés állandó, akkor a minden egyes szavazat leadása után a gép a szavazatot

eljuttatja a feljebb lévő adatbázisba. A másik esetben a gép tárolja egy ideig a szavazatokat és csak egy bizonyos idő elteltével küldi el őket. Ez történhet például 10 percenként, óránként. Nem csak időhöz lehet kötni, akkor is továbbíthatja a szavazatokat, ha egy adott számú voks összegyűlt. A harmadik esetben végig a gép tárolja a szavazatokat, és a szavazás lezajlása után begyűjtik az adatokat az egyes gépekről. Az első és a második megoldás biztonság szempontjából szinte megegyezik. Az adatokat küldhetik interneten keresztül vagy egy közvetlenül erre a célra kifejlesztett hálózaton. Mindkét esetben erősen kódolni kell az adatokat, de a magánhálót nehezebben lehet támadni és gyorsabb is, mint az internet, hiszen más forgalom nincs rajta. Az állandó összeköttetés hátránya, hogy a támadónak sokkal több ideje van próbálkozni az adatok megszerzésére, mint a másik esetben. A magánháló hátránya még, hogy azt ki kell építeni, ami sok időt, pénzt és emberi munkát vesz igénybe. A harmadik megoldás hátránya, hogy igen sok időt és emberi erőforrást vesz igénybe, viszont nehezebben támadható, mint a hálózaton való küldés esetén.

A szavazatok kétféleképp tárolhatóak: vagy minden egyes szavazatot tároljuk, vagy csak a megfelelő jelöltek szavazatszámát növeljük mindig eggyel. Az első megoldás több erőforrást igényel, de ez elhanyagolható költséget jelent. Előnye viszont, hogy pontosan tudjuk, hogy hányan szavaztak és ez fontos információ lehet, amikor a szavazás tisztességességét ellenőrzik.

4.3.2. Protokoll

Mindkét rendszernél, ha a számítógép továbbítja a szavazatokat, a következő protokollt ajánljuk. A szavazó egy bírónak is leadja a szavazatát. A számítógép a szavazatot nem csak a felette lévő adatbázisnak, hanem a bírónak is továbbítja másolatként. Ha a bíró úgy látja, hogy a szavazótól és a számítógéptől kapott szavazat megegyezik, akkor jelzi az adatbázisnak, hogy a szavazat véglegesíthető. Urnazárás után csak a véglegesített szavazatokat számlálják meg. A bíró küld egy igazolást a szavazónak. Ez természetesen nem tartalmazhatja a szavazatot, mert ekkor a szavazó be tudná bizonyítani, hogy kire szavazott.

4.3.3. Meghibásodás

Mint azt már említettük, az elektronikus szavazás egyik problémája a gépek meghibásodása, különösen, ha szavazás közben romlik el egy gép. A gépek állapotától függetlenül a legális szavazatokat figyelembe kell venni, nem szabad egyet sem kihagyni a számlálásnál.

1. *Ha a szavazatok továbbítása azonnal megtörténik:*
   Ha nem szavazás közben hibásodik meg egy gép, az nem nagy baj. Egy másik fülkében továbbra is lehet szavazni. Mivel a rendszer hierarchikus, és a felette lévő szinten is tárolják az adott gépen leadott szavazatokat, ezért az ellenőrizhetőség sem jelent problémát. A komoly probléma az, ha éppen szavazat elküldésekor megy tönkre a gép. Ekkor nem kap visszaigazolást a szavazó, ezért egy másik gépen újra szavazhat. Viszont nem lehet tudni, hogy az sikerült-e elküldeni a szavazatot, vagy már előtte ment tönkre a gép, illetve hogy az elküldött adat helyes-e. Erre a megoldást a bíró és egy átmeneti tár jelenti. A gép által küldött szavazat a központban, egy átmeneti tárban lesz elhelyezve. Amikor a bíró igazolást küld a szavazópolgárnak, akkor egyúttal a központi adatbázisnak is jelzi, hogy az általa ellenőrzött gép utoljára elküldött adata véglegesíthető.

2. *Ha a szavazatok továbbítása nem azonnal történik:*
   A gép bizonyos időközönként kapcsolódik a központhoz és küldi el a felhalmozódott adatokat. Két esetet kell megkülönböztetni. Az egyik, ha a gép akkor hibásodik meg, amikor épp küldi a felhalmozódott szavazatokat. Ilyenkor ugyanúgy kell eljárni, mint az előbb. A másik eset, ha akkor hibásodik meg, amikor nincs kapcsolatban a központtal. Ha akkor hibásodik meg, amikor senki sem szavaz, akkor csak a felhalmozódott adatot kell kinyerni a gépből. A szavazatokat tároló elemet kell áthelyezni egy megfelelő gépbe, esetleg a központba, és onnan kiolvasni az adatokat Ez csak nagyon kivételes esetben nem lehetséges (például az adathordozó megsemmisül, vagy meghibásodik). Ezenkívül felmerül még a kérdés, hogy honnan tudjuk, hogy az elemen talált adatok helyesek-e. Nos ezt nem tudhatjuk, hiszen a szavazás titkos. Csak annyit tehetünk, hogy nem egyszer, hanem többször és több helyen tároljuk a szavazatokat, pl. háromszor három tárolón. Így ha az egyik meghibásodik, akkor még mindig lehet használni a másikat (elég kicsi a valószínűsége, hogy mindhárom meghibásodik). Ezen kívül összevethetjük a tárolók tartalmát, és többségi döntéssel eldönthetjük, hogy az adatok helyesek-e vagy sem.

4.4. Adatvédelem

A személyes adatok kezelésének és védelmének követelményeit a fenti két rendszer magas szinten teljesíti.

A szavazóhelyiségben tartózkodó bizottság, őrség nem tudja, hogy ki a szavazó, mivel előttük nem kell magát azonosítania a választónak. Sőt, az sem mondható meg a

választások után, hogy ki szavazott, és ki nem. Ma ez megmondható, hiszen aki kapott szavazólapot, az a bizottságnál hagyja a kézjegyét. A véleménynyilvánítás továbbra is fülkében történik, mások által nem látható módon. A rendszer nem párosítja, és nem is tudja párosítani a szavazó adatait és szavazatát, vagyis teljesül a titkosság követelménye.

Ha eltekintünk a helyi választókerületi választói névjegyzék helyben szokásos kifüggesztésének ellenőrző funkciójától (tehát attól, hogy a választópolgárok ellenőrizhessék a szavazásra jogosultak körét és egyben saját nevük feltüntetését), akkor az ismertetett rendszerek arra is alkalmasak, hogy a szavazási joguktól a szavazást közvetlenül megelőzően megfosztottak esetében is adatvédelmileg korrekt eljárást biztosítsanak. Elképzelhető ugyanis, hogy valaki rendelkezik kártyával, de nem jogosult a szavazásra. Például átvette a szavazás napja előtt a kártyáját, de a szavazás napjára a közügyektől már eltiltották. Ebben az esetben a következő eljárás alkalmazható: a választásra nem jogosult ember is bemehet a fülkébe, de azonosítása után a rendszer nem regisztrálja a szavazatát. Ez hasonló ahhoz az eljáráshoz, ami már megszokott a véradásnál: a fertőzött véradó is ad vért, csak a papírok kitöltésénél jelzi betegségét, így az ő vérét külön teszik majd és a többi véradó előtt nem kell felfednie a betegségét.

Az elektronikus szavazórendszerektől elvárt — korábban ismertetett — feltételek is teljesülnek:

- A rendszer csak a szavazásra jogosultak szavazatát veszi figyelembe — *pontosság*.
- Mindenki csak egyszer szavazhat, és csak akkor, ha van hozzá joga, senki sem szavazhat másik szavazó nevében — *demokratikusság*.
- Senki sem tudja összepárosítani a szavazatokat és a szavazókat, és egyetlen szavazó sem tudja sem bebizonyítani, hogy kire szavazott — *titkosság*.
- A fülkében lévő gépektől kezdve minden hierarchiaszinten a gépek tárolják a szavazatokat, és csak a szavazatokat, és esetleg azt, hogy melyik gépnél adták le azokat. Ez elegendő az újraszámlálhatósághoz, illetve ahhoz, hogy ne lehessen utólag szavazatokat becsempészni az adatbázisokba — *ellenőrizhetőség*.
- A szavazók a lehető legegyszerűbben, néhány gomb megnyomásával szavazhatnak — *egyszerűség*.
- Akárhány jelöltet fel lehet sorolni, akármilyen bonyolult kérdést fel lehet tenni — *rugalmasság*.
- A rendszert akármelyik fülkében, akármelyik településen ki lehet építeni — *mobilitás*.
- Urnazárás után szinte azonnal meg lehet számolni a szavazatokat — *gyorsaság*.

Mint már említettük, a rendszert felügyelőknek, kifejlesztőknek több lehetősége van a csalásra. A sikeres támadás esélye csökkenthető, ha semmilyen indokkal sem férhet a rendszerhez egyedül egy felügyelő. Ma már alkalmaznak olyan megoldásokat, amikor több rendszergazda van, de mindegyik különböző jogosultságokkal. Létezzen háromféle rendszergazda: az egyik csak a belépéshez ad jogot a kártyájával, a másik csak a fülkében lévő számítógéphez férhet hozzá az azonosító kártyájával, a harmadik pedig csak a biometrikus azonosító készülékekhez. Így bármilyen meghibásodás esetén legalább két ember illetve kártya kell a hiba orvoslásához: a belépéshez jogot adó kártya és az adott egységhez való hozzáféréshez szükséges kártya.

Egy elektronikus szavazórendszer kiépítéséhez sok pénzre van szükség. Venni kell szavazógépeket, esetleg ki kell építeni egy hálózatot. Az első ismertetett esetben kapukat is kell gyártani, a második esetben intelligens kártyákat kell készíteni (esetleg mindkettőt). Lássuk viszont, mit spórolunk ezzel? Elsősorban rengeteg időt, energiát és emberi munkát. Ezenkívül sok papírt, tintát és nyomdaköltséget. Egy lengyel tanulmány[13] szerint, ha Lengyelországban bevezetnék az ATM-szerű szavazógépeket, akkor a gépekre költött pénz megegyezne azzal az összeggel, amit négy év alatt papírra és nyomtatásra költenének.

4.5. Nem szavazóhelyiségből történő szavazás

A nem szavazóhelyiségből történő szavazás több komoly problémát vet fel, amelyekre tudomásunk szerint még nem születtek alapos, kimerítő megoldások. Otthoni szavazásnál a választónak, munkahelyi szavazásnál a munkáltatónak kell beszereznie a szükséges szoftvereket és hardvereket. Ezek költségesek, ráadásul hitelesíttetni kell őket. Hiába bármilyen azonosítás, azzal csak az garantálható, hogy egy szavazásra jogosult polgár legálisan szavazásra jelentkezett. Azt senki sem biztosíthatja, hogy a szavazata valóban a bejelentkező véleményét tükrözi, ítélőképessége birtokában, szabad akarata szerint szavazott.

Ha valaki nem otthonról szavaz, akkor a szavazata átmegy a munkahelyén, vagy a netkávézó egy-két tűzfalán, ami adatvédelmi és adatbiztonsági szempontból egyaránt aggályos. Az internet hatalmas és nyílt rendszer. Ebből kifolyólag bárki hozzáférhet szinte bármelyik pontjához. Semmilyen elfogadható biztonsági garancia nincs arra, hogy megérkezik, és módosítások nélkül időben érkezik meg a feladó küldeménye a címzetthez. Egy szavazásnál pedig akár egyetlen szavazat is döntő lehet.

[13] Maciej Janiec és Mateusz Drożdż: E-voting, elektroniczne systemy głosowania (http://www.markom.krakow.pl/~mjaniec/pdf/e-voting.pdf)

4.6. Az elektronikus szavazás helyzete Magyarországon

Jelenleg a hazai jogrend nem ismeri az elektronikus szavazás fogalmát, így az Országos Választási Iroda nem is tervezhet, pályáztathat elektronikus szavazórendszert.

2003 őszén az Országgyűlés elé került egy törvénytervezet, melyben szerepel az elektronikus szavazás. A tervek szerint 2004 júniusában, az Európai Parlamenti választásokon hazánk külképviseleteiről elektronikus úton, elektronikus szavazógéppel nyilváníthattak volna véleményt az erre jogosult állampolgárok. Az MSZP Informatikai Csoportja meg is tervezett egy gépet, mely szerintük minden követelménynek megfelel. Az Országgyűlés ezt a törvénytervezetet nem szavazta meg, helyette 2003 decemberében fogadták el azt az EP választásokról szóló törvényt, amely nem ismeri el az elektronikus szavazást, így itthon és a külképviseleteinken is a hagyományos módon élhettek a szavazópolgárok alkotmányos jogukkal. Az Országos Választási Iroda tájékoztatása szerint az EP választásokon 100 tonna papírt, 60 ezer tollat és 200 km hosszú nemzeti színű szalagot használtak fel.

2004 áprilisában a kormány a belügyminiszter előterjesztésében benyújtotta a Parlamentnek a T/9843. számú törvényjavaslatát a választási eljárásról szóló 1997. évi C. törvény módosításáról.[14] A javaslat szerint a jövőben a külképviseleteken elektronikus úton lehet majd szavazni:

„126/B. § (3) A külképviseleti szavazás a külképviseleten elhelyezett szavazógép segítségével, a szavazás titkosságát biztosító módon történik. A szavazógép biztosítja a szavazat kizárólagosságát, egyszeriségét, anonimitását, pontosságát, valamint a szavazófülkében a szavazó által történő felülbírálhatóságát. A szavazógép használatának módja garantálja a szavazás törvényességét és a szavazat leadásának kényszermentességét. A külképviseleten történő szavazásra a szavazóhelyiségben nem kell urnát felállítani."

Ezt a módosító törvényjavaslatot az előterjesztő 2004. október 11-én átdolgozásra visszavonta. Hatályba lépése esetén ez a törvényi rendelkezés vezette volna be az elektronikus szavazás fogalmát a hazai jogrendbe, és a mi rendszereinkhez hasonló rendszert írt volna elő a külképviseleteken történő választások esetére.

[14] Lásd az Országgyűlés honlapján, a http://www.mkogy.hu/irom37/9843/9843.htm oldalon.

5. Összefoglalás

Tanulmányunkban két olyan elektronikus szavazási rendszer koncepcióját ismertettük, amely a biometrikus rejtjelezés, technikailag a bioszkript alkalmazásán alapul. Megoldásainkat eredetinek tartjuk; forráskutatásaink során hasonló rendszer leírásával nem találkoztunk.

Fontosnak tartjuk hangsúlyozni, hogy az ismertetett rendszerek lényege, hogy nem központilag tárolt, személyazonosításra alkalmas biometrikus azonosítók (például ujjlenyomatok) használatán alapulnak, hanem a szavazásra jogosultak biometrikus adataiból származtatott és így harmadik személyek számára értelmezhetetlen, de a szavazási jogosultságot egyértelműen bizonyító bioszkript használatán. Ezzel biztosíthatók a képviselőválasztások és népszavazások titkossági, biztonsági és egyéb alapvető feltételei.

A rendszerek további előnye, hogy alkalmazásukkal magas szinten teljesíthetők a személyes adatok védelmének jogi és technológiai követelményei, köztük is kiemelten a célhozkötöttség, vagyis az, hogy az adatkezelési célhoz szükséges és elégséges mértékű és időtartamú adatkezelés történjék.

Források

A szavazással, választásokkal kapcsolatos magyar jogi anyagok:

www.valasztas.hu

Biometria, bioszkript:

Colin Soutar: Biometric System Security

Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, és B.V.K. Vijaya Kumar: Biometric Encryption™

(www.bioscrypt.com)

PET:

www.cdt.org/privacy

Székely Iván: PET technológiák: a személyes adatok védelmének korszerű eszközei. In: *Létezik-e adatvédelem adatbiztonság nélkül?* Infoszféra Kft., Budapest 2000.

Elektronikus szavazásban használt protokollok:

Farrel Lifson: The Security of Electronic Online Voting
(http://people.cs.uct.ac.za/~flifson/things/security/essay.html)

Sensus:

http://lorrie.cranor.org/voting/sensus/

Hírek, tanulmányok az elektronikus szavazásról:

http://www.magyarorszag.hu/eu/hirek/elektrvalaszt20030710.html

http://www.notablesoftware.com/evote.html

http://news.bbc.co.uk/1/hi/talking_point/1746785.stm#top

http://www.ittk.hu/infinit/

http://computer.howstuffworks.com/e-voting.htm

http://www.democracynow.org

http://www.cnn.com/

http://www.dailyvanguard.com/

http://www.theregister.co.uk/

Lorrie Faith Cranor: Electronic Voting — Computerized polls may save money, protect privacy (1996, ACM Crossroads Student Magazine)
(http://www.acm.org/crossroads/index.html)

Lorrie Faith Cranor: Voting After Florida: No Easy Answers, 2001. március 19.
(http://lorrie.cranor.org/voting/hotlist.html)

Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin és Dan S. Wallach: Analysis of an Electronic Voting System, 2003. július 23. (http://avirubin.com/vote.pdf)

Maciej Janiec és Mateusz Drożdż: E-voting, elektroniczne systemy głosowania
(http://www.markom.krakow.pl/~mjaniec/pdf/e-voting.pdf)

Függelék

A. A biometrikus rejtjelezés algoritmusa[15]

A biometrikus rejtjelező algoritmus az ujjlenyomat teljes képét felhasználja, ellentétben sok más rendszerrel, amelyek az ujjlenyomatnak csak egy részét vagy különböző pontjait használják az azonosításhoz. Az algoritmus a korrelációra épül. A korrelációt következőképp használják fel biometriát használó rendszerek esetében. A kétdimenziós bemeneti képet az egyszerűbb áttekinthetőség kedvéért az egyváltozós f(x) reprezentálja, ennek Fourier-transzformáltja (a frekvenciatartományban) F(u), definíció szerint:

$$F(u) = \int_{-\infty}^{\infty} f(x) e^{-jux} dx \qquad \text{(Az inverz Fourier-transzformáció:} \qquad f(x) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F(u) e^{jux} du \quad)$$

A reprodukált ujjlenyomatot egy az adatbázisban tárolt ujjlenyomattal hasonlítják össze. Az adatbázisban legelőször tárolt képet $f_0(x)$ reprezentálja. $f_1(x)$ egy későbbi kép, amit azonosításkor olvasunk be. H(u), a szűrésre használt függvény, $f_0(x)$-ből van származtatva. A korreláció $f_0(x)$ és $f_1(x)$ között c(x), ami a következőképpen néz ki:

$$c(x) = \int_{-\infty}^{\infty} f_1(v) f_0^*(x + v) dv$$

ahol * a komplex konjugált. A gyakorlatban a rendszer kimenetét F1(u) és F0*(u) inverz Fourier-transzformáltja adja:

$$c(x) = FT^{-1}\left\{F_1(u) F_0^*(u)\right\}$$

ahol F_0*(u)-t H(u)-val helyettesítik. A korrelációra épülő, biometriát használó rendszerek H(u)-hoz hasonlítják a beolvasott ujjlenyomatot. H(u) úgy van megtervezve, hogy a rendszer kimenetén egy korrelációs csúcs jelenjen meg.

Ezek után nézzük meg, hogyan használja ezt ki a bioszkript. Mint láttuk, a korrelációt használó algoritmus válasza csak annyit tud jelezni, hogy az ujjlenyomat legális felhasználóé-e vagy sem. A bioszkriptnek egy jellemzően 128 bites információra is szüksége van, ez lesz a nem biometrikus adat, a digitális kulcs. Ráadásul ezt úgy kell megvalósítani, hogy egyrészt egy legális felhasználót akkor is felismerjen a rendszer, ha deformálódott az ujjlenyomata, nedvesebb a keze stb., másrészt pedig ha egy támadó próbál használni egy bioszkriptet, akkor a rendszer használhatatlan 128 bites kulcsot adjon válaszul. Az első cél elérhető úgy, hogy nem egy, hanem több ujjlenyomat alapján határozzuk meg H(u)-t. Vagyis van T≥1 darab ujjlenyomatunk $\{f_0^1(x), f_0^2(x), \ldots, f_0^T(x)\}$.

[15] Eredeti közlemény: Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, és B.V.K. Vijaya Kumar: Biometric Encryption. In: Randall K. Nichols (ed.): *ICSA Guide to Cryptography,* Chapter 22, McGraw-Hill 1999, http://www.bioscrypt.com/assets/Biometric_Encryption.pdf

A rendszer $f_0^t(x)$-re adott válasza $c_0^t(x)$. A kívánt válasz legyen r(x). A rendszer válasza c(x), ez lesz felhasználva a bioszkript előállításakor és a digitális kulcs kinyerésekor is. Így azt szeretnénk, hogy 1>t>T esetén $c_0(x)^t \approx r(x)$ teljesüljön, vagyis hogy a kimenet minél jobban hasonlítson a kívánt kimenetre minden $f_0^t(x)$-re.

Legyen

$$\mathrm{E_H} = \frac{1}{\mathrm{T}} \sum_{t=1}^{T} \int \left| c_0^t(x) - r(x) \right|^2 dx$$

a hiba mértéke, vagyis $E_H=0$, ha $c_0^t(x) = r(x)$.

Legyen

$$\mathrm{E_T} = \int |H(u)|^2 P(u) du$$

a torzítás mértéke, ahol P(u) az ujjlenyomatok közti váltás teljesítmény spektruma:

$$\mathrm{P(u)} = \frac{2}{T(T-1)} \sum_{t=1}^{T-1} \sum_{s=t+1}^{T} \left| \mathrm{FT}\left\{ \varepsilon_{bejövő}^{t,s}(x) \right\} \right|^2$$

$\varepsilon_{bejövő}$ jelentése:

$$\mathrm{f_0^t}(x) = \mathrm{f_0^s}(x) + \varepsilon_{bejövő}^{t,s}(x)$$

minden $s,t \in \{1,\ldots T\}$, és $t \neq s$-re. Célunk pedig, hogy az előbbi egyenlet alapján meghatározott $f_0^t(x)$ esetén

$$\mathrm{c_0^t}(x) = \mathrm{c_0^s}(x) + \varepsilon_{kimenő}^{t,s}(x)$$

legyen minden $s,t \in \{1,\ldots T\}$, és $t \neq s$-re.

Vagyis E_H-tól függ, hogy mennyire szelektál a rendszer, milyen pontosan tudja megkülönböztetni a felhasználókat egymástól és a támadóktól, és E_T-től függ, hogy mennyire toleráns a rendszer a beolvasott ujjlenyomatok deformációjára. Olyan H(u)-t szükséges választani, ami minimalizálja az összes hibát. Ezt a következő összefüggés segítségével tehetjük meg ($0 < \alpha < 1$):

$$\mathrm{E} = \alpha \mathrm{E_T} + \sqrt{1-\alpha^2}\,\mathrm{E_H}$$

Így α értéke határozza meg az E_H és E_T közötti kompromisszumot. Az eddigi összefüggések alapján H(u)-t a következő képlet alapján számolhatjuk (* a komplex konjugált, R(u) pedig r(x) Fourier transzformáltja):

$$\mathrm{H(u)} = \sqrt{1-\alpha^2}\, \frac{\left[\frac{1}{T} \sum_{t=1}^{T} F^{*t}{}_0(u) \right] R(u)}{\left\{ \alpha P(u) + \sqrt{1-\alpha^2}\, \frac{1}{T} \sum_{t=1}^{T} \left| F_0^t(u) \right|^2 \right\}}$$

Vezessük be a következő változókat:

$$\mathrm{A}_0(u) = \frac{1}{T}\sum_{t=1}^{T} F_0^t(u) \qquad \mathrm{D}_0(u) = \frac{1}{T}\sum_{t=1}^{T} \left|F_0^t(u)\right|^2$$

H(u) képletében az $\sqrt{(1-\alpha^2}$ -es szorzó elhanyagolható (mivel, ahogy később majd látjuk, csak fázist fogunk tárolni, amit ez a konstans szorzó nem befolyásol):

$$\mathrm{H(u)} = \frac{\mathrm{A}_0^*(u)R(u)}{\alpha P(u) + \sqrt{1-\alpha^2}D_0(u)}$$

Tehát az, hogy a rendszer mire érzékeny, α-tól függ. Ha α=0, akkor a rendszer nagyon szelektál, de nem tolerálja a deformációt. Ha α=1, akkor a rendszer nagyon toleráns a deformációval szemben, de nehezen fogja azonosítani a felhasználókat. Így kialakítva H(u) optimális bármilyen R(u)-ra.

Eddig két követelményt teljesít a rendszer, a következő lépés a harmadik teljesítése, vagyis hogy sem a biometrikus adatot (f(x)), sem a nem biometrikus adatot (r(x)) ne lehessen kinyerni a bioszkriptből. Logikus lenne H(u)-t, mint bioszkriptet tárolni, de még nagyobb biztonság érhető el, ha H(u) egy módosított változatát tároljuk, legyen ez $\mathrm{H_M(u)}$. $\mathrm{H_M(u)}$ akkor a legbiztonságosabb, ha H(u)-nak csak a fázis komponense van tárolva: $e^{i\phi_H(u)}$. Ilyenkor R(u) egy random, egyenletes eloszlású fázis függvény lesz. Viszont H(u)-nak nem csak fázisa, hanem amplitúdója is van, amit nem tárolunk, így a tárolt és az optimális függvény nem egyezik meg.

Ennek a problémának a megoldása az, hogy az amplitúdót tárolás helyett minden egyes azonosításnál újra előállítjuk. Tegyük fel, hogy olyan R(u)-t generálunk, amely elemeinek amplitúdója egységnyi, fázis értékei pedig random és egyenletes eloszlásúak, vagyis $0 \le j < 2\pi$, például:

$$R(u) = e^{i\phi_R(u)} = e^{i2\pi \cup [0,1)}$$

ahol U[0,1) minden m eleme random és egyenletes eloszlású úgy, hogy $0 \le m < 1$. Így R(u) helyére az előző egyenletben megadott alakot írva:

$$H(u) = \frac{A_0^*(u)}{\alpha P(u) + \sqrt{1-\alpha^2}D_0(u)} e^{i\phi_R(u)}$$

ennek alapján:

$$c_0^t(x) = FT^{-1}\left\{ F_0^t(u) \frac{\left| A_0(u) e^{-i\phi_{A_0}(u)} \right|}{\alpha P(u) + \sqrt{1-\alpha^2} D_0(u)} e^{i\phi_R(u)} \right\}$$

illetve:

$$c_1^t(x) = FT^{-1}\left\{ F_1^t(u) \frac{\left| A_0(u) e^{-i\phi_{A_0}(u)} \right|}{\alpha P(u) + \sqrt{1-\alpha^2} D_0(u)} e^{i\phi_R(u)} \right\}$$

A cél, hogy $c_1^t(x)$ és $c_0^t(x)$ a lehető legjobban hasonlítson. Mivel ezek függnek az ujjlenyomat képétől ($f_1^t(x)$-től és $f_0^t(x)$-től), akkor lesznek identikusak, ha a két ujjlenyomat, amiből $f_1^t(x)$-et és $f_0^t(x)$-et nyerik, teljesen azonos, ami szinte lehetetlen. Viszont ahogy T növekszik, úgy konvergál $A_0(u)$ egy adott függvényhez, így T=6 esetén $A_1(u) \cong A_0(u)$ és $D_1(u) \cong D_0(u)$. Így az előző egyenletekben $F_0^t(u)$-t $A_0(u)$-val, $F_1^t(u)$-t $A_1(u)$-val helyettesíthetjük (vagyis az ujjlenyomatokat az ujjlenyomatok átlagával helyettesítjük). Mivel az amplitúdót nem tároljuk, ezért $|A_0(u)|$-t $|A_1(u)|$-val, $D_0(u)$-t pedig $D_1(u)$-val helyettesíthetjük, így:

$$c_0(x) = FT^{-1}\left\{ A_0(u) \frac{\left| A_0(u) \right| e^{-i\phi_{A_0}(u)}}{\alpha P(u) + \sqrt{1-\alpha^2} D_0(u)} e^{i\phi_R(u)} \right\}$$

$$= FT^{-1}\left\{ A_0(u) \frac{\left| A_0(u) \right|}{\alpha P(u) + \sqrt{1-\alpha^2} D_0(u)} e^{-i\phi_{A_0}(u)} e^{i\phi_R(u)} \right\}$$

$$= FT^{-1}\left\{ A_0(u) \bullet \left| H_0(u) \right| \bullet H_M(u) \right\}$$

és

$$c_1(x) = FT^{-1}\left\{ A_1(u) \frac{\left| A_1(u) \right| e^{-i\phi_{A_0}(u)}}{\alpha P(u) + \sqrt{1-\alpha^2} D_1(u)} e^{i\phi_R(u)} \right\}$$

$$= FT^{-1}\left\{ A_1(u) \frac{\left| A_1(u) \right|}{\alpha P(u) + \sqrt{1-\alpha^2} D_1(u)} e^{-i\phi_{A_0}(u)} e^{i\phi_R(u)} \right\}$$

$$= FT^{-1}\left\{ A_1(u) \bullet \left| H_1(u) \right| \bullet H_M(u) \right\}$$

Mivel csak a fázis és a komplex konjugált kerül tárolásra:

$$H_M(u) = e^{-i\phi_{A_0}(u)} e^{i\phi_R(u)}$$

$H_M(u)$ tárolását úgy kell megoldani, hogy ne lehessen belőle visszanyerni sem f(x)-et, sem r(x)-et. Ezt az úgynevezett „fázis-fázis termék" koncepcióval oldották meg. Ez a megoldás a one-time pad kriptográfiai eljárással rokon. A one-time pad definíciója: $P=C=K=\{0,1\}^n$, ahol $n\geq 1$. A kódolás úgy történik, hogy 2 n bites bináris sztringet (az eredeti szöveg — plain text és a kulcs — key) modulo 2 összeadják, az eredmény a kódolt információ — ciphertext. A dekódolásnál a kódolt szöveget és a kulcsot adják össze modulo 2 és az eredmény az eredeti szöveg lesz. P az eredeti szöveg (**P**lain text), C a kódolt információ (**C**iphertext), K pedig a kulcs (**K**ey). Mivel a kódoláshoz használt kulcsot random és csak egyszer használják, ezért ez a fajta kódolás teljes biztonságot nyújt. A fázis-fázis terméket a következőképp állítják elő: két fázis szint van, a 0 és a π. $P=C=K=\{0, \pi\}^n$, ahol $n\geq 1$.

A kódolás definíció szerint két fázisokból álló sor terméke:

$$e^{i\phi_p} \bullet e^{i\phi_k} = e^{i\phi_c}$$

ahol $\phi_p \in P$, $\phi_k \in K$ és $\phi_c=\phi_p+\phi_k \pmod{2\pi}$.

A dekódolás definíciója:

$$e^{i\phi_c} \bullet e^{-i\phi_k} = e^{i\phi_p}$$

ahol $\phi_p=\phi_c-\phi_k \pmod{2\pi}$.

Mivel $(-\phi_k)\equiv\phi_k \pmod{2\pi}$, ezért a képlet:

$$e^{i\phi_c} \bullet e^{i\phi_k} = e^{i\phi_p}$$

A bináris fázis-fázis termék elemei: e^{i0}, $e^{i\pi}$, és a következő érvényes rájuk:

$$e^{i0} \bullet e^{i\pi} = e^{i\pi} \bullet e^{i0} = e^{i\pi}$$
$$e^{i0} \bullet e^{i0} = e^{i\pi} \bullet e^{i\pi} = e^{i0}$$

Ha Γ egy ilyen transzformáció: $\Gamma\ \{ e^{i0} \rightarrow 0, e^{i\pi} \rightarrow 1, \bullet \rightarrow \oplus\}$, akkor az egyenletek átírhatóak a következő alakba: $0 \oplus 1 = 1 \oplus 0 = 1$, $0 \oplus 0 = 1 \oplus 1 = 0$, ami éppen a one-time pad eljárással egyezik meg. Ebből következik, hogy a fázis-fázis termék is teljes biztonságot nyújt, ha a kulcs random és csak egy felhasználó felvételéhez használják. Bizonyítható, hogy ez a biztonság akkor is fennáll, ha tetszőleges számú fázis szintet használnak. Mivel $H_M(u)$ egy fázis-fázis termék, ahol a random és egyszer használt kulcs $e^{i\phi_R(u)}$, ezért fennáll a teljes biztonság.

B. A felismerő algoritmus biztonsága

A rendszer biztonsága attól függ, hogy a rendszer mennyire engedi különbözni $c_1(x)$-et $c_0(x)$-től. A már meghatározott egyenlőségek:

$$c_0(x) = FT^{-1}\left\{ A_0(u)e^{i\phi_{A_0}(u)} \bullet \frac{|A_0(u)|}{\alpha P(u) + \sqrt{1-\alpha^2}\, D_0(u)} \bullet \left[e^{-i\phi_{A_0}(u)} e^{i\phi_R(u)} \right] \right\}$$

$$c_1(x) = FT^{-1}\left\{ A_1(u)e^{i\phi_{A_1}(u)} \bullet \frac{|A_1(u)|}{\alpha P(u) + \sqrt{1-\alpha^2}\, D_1(u)} \bullet \left[e^{-i\phi_{A_0}(u)} e^{i\phi_R(u)} \right] \right\}$$

ahol

$$\left[e^{-i\phi_{A_0}(u)} e^{i\phi_R(u)} \right] = H_M(u)$$

Ha egy legális felhasználó azonosítja magát, akkor: $A_1(u) \approx A_0(u)$, $D_1(u) \approx D_0(u)$ és $e^{i\phi_{A_1}(u)} \bullet e^{-i\phi_{A_0}(u)} \approx 1$, így egyedül $e^{i\phi_R(u)}$, a random előállított adat az, ami $c_1(x)$ értékét alakítja.

Ha egy támadó próbálkozik a belépéssel, akkor: $A_1(u) \neq A_0(u)$, $D_1(u) \neq D_0(u)$ és $e^{i\phi_{A_1}(u)} \bullet e^{-i\phi_{A_0}(u)} \neq 1$, így nemcsak $e^{i\phi_R(u)}$, hanem a többi együttható ($A_1(u)$ stb.) is befolyásolja $c_1(x)$ értékét. Ez azt jelenti, hogy $c_1(x)$ jelentősen el fog térni $c_0(x)$-től és az ebből nyert kulcs nem fog megegyezni azzal a kulccsal, amit a legális felhasználó felvételekor csatoltak.