Egy ideális anonim digitális pénzrendszer

Tóth Csaba*

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
e-mail: tocsa@dc.sote.hu

„Those who are willing to sacrifice freedom in the name of security will have neither."
(Benjamin Franklin)

Absztrakt

E tanulmány célja, hogy széleskörűen és rendszerszemléletűen vizsgálja a létező digitális pénzrendszerek tulajdonságait, ezek között kiemelten az anonimitást, mint a személyes adatok védelmének eszközét, valamint a biztonság különböző aspektusait; továbbá hogy összegezze egy ideális rendszerrel szemben elvárható követelményeket. A digitális pénz séma mibenlétének meghatározása után a szerző áttekinti a Chaum kutatásaiból kiinduló evolúciós folyamatot, ennek főbb állomásait és jellemzőit. Ennek során számos, sokféle célra használható sémát és technológiát mutat be, köztük kreatív és új kriptográfiai primitíveket, amelyek alapvető építőelemként lehetnek jelen a sémákban, vagy pedig modulárisan biztosíthatnak kívánt tulajdonságokat. Hivatkozik a sémák tudományos publikációira és elemzi az összehasonlító művek által fontosnak tartott tulajdonságokat. Esetenként eltérő csoportosításban vagy más aspektusból tekint bizonyos tulajdonságokat, olyan részletesen felbontva a biztonság és az anonimitás tulajdonságokat, ahogy az a szakirodalomban eddig nem szerepel. Ezek tárgyalása közben számos olyan kísérleti digitális pénz sémát elemez, amelyeket más művek nem vetettek össze vagy vizsgáltak meg. Ezt követően a szerző sorra veszi, hogy egy elképzelt ideális digitális pénzrendszernek milyen tulajdonságokat kell teljesítenie. Kiemeli, hogy megítélése szerint mely fő problémák nyitottak az egész kutatási terület előtt és szubjektív kitekintést ad a várható fejlődésről.

Kulcsszavak: *anonimitás, digitális pénz, kriptográfia, biztonság, fizetési sémák*

* Tóth Csaba, műszaki informatikus, a BME GTK Információ- és Tudásmenedzsment Tanszékén diplomázott okleveles bankinformatikus szakmérnök.

1. Bevezető

Az elektronikus pénz protokollok tudománya multidiszciplináris terület. A kriptográfia mellett nagy szerepet kap a tranzakció tudománya, az adatbázis-elmélet, a számítógépes hálózatok tudománya és más tudományágak. Fontosak a gazdasági, banki és jogi vetületek is. E tanulmány főként a kriptográfiai, az adatvédelmi és az adatbiztonsági vetületekre koncentrál.

Amellett, hogy multidiszciplináris területet képviselnek, a pénz protokollok igen sokszínűek és szerteágazók. Az „elektronikus fizetési rendszerek" kifejezés igen tág fogalom. Magában foglal szinte mindent, például a hagyományos bankkártyás credit/debit tranzakciós rendszereket, az elektronikus csekk rendszereket, az ATM (Automated Teller Machine) tranzakciókat vagy POS (Point Of Sale) terminálos fizetéseket. Megítélésem szerint ezek kellőképpen publikált és kutatott területek, ezért nem ezekkel szeretnék foglalkozni. Az elektronikus fizetési rendszerek egy részterületét képezik a digitális pénzrendszerek, melyek jóval hasonlatosabbak a valódi pénzhez, mint korábban említett rokonaik. A digitális pénzek esetén a felhasználó digitális pénztárcájában (általában speciális programozású, nehezen feltörhető smart card) jelen van egy olyan bitsorozat, ami önmagában értéket tud képviselni, tulajdonképpen egy digitális pénzérme. Nem mindig jelenik meg explicit pénzérme, léteznek olyan rendszerek, amelyeknél csak egy számláló található a pénztárcában, és ez a számláló mutatja a tárcában található aktuális pénzösszeg mennyiségét. A digitális pénz területét is célszerű még tovább szűkíteni, mert még ezen belül is vannak olyan részterületek, amelyek önmagukban is jelentős vizsgálati terepet képviselnek. Erre jó példa a mikrofizetési rendszerek, amelyek kis értékű fizetések gazdaságos véghezvitelét is lehetővé teszik. A mikrofizetési rendszereknél a kutatók — szándékuk ellenére — kénytelenek apró kompromisszumokat kötni a hatékonyság növelése és az algoritmikus költségek csökkentése érdekében, és ez a rendszer biztonságának instabilabb alapokra helyezését, a rendszer nehezebb bizonyíthatóságát, vagy megengedőbb peremfeltételekkel való bizonyíthatóságát, s ezáltal a biztonsági kockázatok növekedését eredményezi.

E tanulmány középpontjában azon digitális pénz protokolloknak egy csoportja áll, melyek gyökerének a Chaum nevével fémjelzett munkák tekinthetők. Ha tanulmányozzuk az irodalmat, akkor kirajzolódik előttünk egy ebből kiinduló fejlődési út. Ennek az útnak bemutatom az egyes állomásait és az azokhoz kapcsolódó bizonyos protokollokat és technikákat.

Több szempontból is fontosnak tartom ezeket a protokollokat. Az egyik szempont, hogy az ezeket publikáló közösségnek igen erős a kriptográfiai bázisa, ami egy későbbi sikeres elektronikus pénzrendszer biztonságának, anonimitásának eléréséhez döntő fontosságú tényező. Ez a közösség bizonyította, hogy a szakértelme mellett igen kreatív is, képes olyan új matematikai és kriptográfiai eszközöket feltalálni, amelyekkel legyőzhetőek a felmerülő problémák.

Több okból is az lenne az üdvözítő, ha a leendő ideális pénz protokolloknak az ilyen sémák képeznék az alapkövét. A kutatók ugyanis a legfontosabbnak a biztonságot és a személyes adatok védelmét tartják. Alapvetően mindig úgy állnak hozzá a tervezéshez, hogy kompromisszumoktól mentes adatbiztonságot és adatvédelmet szeretnének. Jóllehet elméleti és gyakorlati okok miatt a tökéletesség eleve nem lehetséges, de egy üzleti vállalkozás ehhez képest más értékrendet képvisel. Egy bank vagy egy kereskedő szemszögéből nézve nagyobb hangsúlyt kapna a kivitelezhetőség, a gazdaságosság, a profitabilitás. Az utóbbi tulajdonságok mind az adatbiztonság és adatvédelem ellen hatnak. Mivel a csalások elkerülése miatt az adatbiztonság a bank érdeke is, ezért valószínűleg gondoskodik annak megfelelő szintjéről (bár sokszor ez sem igaz), azonban nincs kielégítő biztosíték arra, hogy megfelelő adatvédelmet nyújtson ügyfelei személyes adatainak kezelése szempontjából.

A kísérleti protokollok néhány kivételtől (DigiCash e-cash) eltekintve csak laborokban vagy esetleg csak elméletben léteznek, nem kaptak jelentős támogatást azoktól a cégektől, amelyek tőkeerősek és nagy felhasználói bázissal bírnak. A hitelkártyacégek és bankok más jellegű, saját kártyás rendszerükhöz közelebb álló megoldásokat próbálnak kutatni. Hogy e két fő kutatási irányból eddig miért nem járt egyik sem átütő sikerrel, azt sokan kutatják.

A jelen tanulmányban érintett legtöbb területet részletesen, bár némiképp más szemszögből tárgyalom bankinformatikus posztgraduális diplomamunkámban [Tót03].

2. A digitális pénz

A digitális pénz lényegében a papírpénz digitális megfelelőjének tekinthető. Kicsit pontosabban fogalmazva a digitális pénz egy olyan információdarab, aminek értéke van. Ezt az információdarabot elfogadják a kereskedők áruért vagy szolgáltatásért cserébe. A valódi digitális pénz az értéket önmagában hordozza, és nem csupán reprezentál egy bankszámlán vagy kredit kártya számlán elhelyezkedő összeget.

A papírpénz előnye, hogy a fizetés nagyon egyszerű vele, a vásárlás eredménye azonnal látható. A papírpénz személytelen, biztosítja a fizető anonimitását, magánéletének

védelmét, átadható bárkinek. Ugyanakkor könnyen ellophatják vagy elveszthetjük, a pénz kezelése költséges, a pénzváltás problémát jelenthet. A papírpénzt széles körben használják illegális ügyletekben. Érdekes hátránya a hagyományos készpénznek, hogy szennyezett lehet és ezáltal betegségeket is terjeszthet.

A digitális pénz célja, hogy kiküszöbölje a hagyományos papírpénz hátrányait, megőrizze annak előnyeit, és emellett újabb előnyös tulajdonságokkal ruházza fel. A digitális pénz biztonságát PIN kód védi, a kezelése olcsóbb, távoli fizetéseket tesz lehetővé (például az interneten keresztül). Fizikailag tiszta. Ha fel van ruházva olyan tulajdonsággal, akkor átadható más, akár távoli felhasználónak is, nem jelent problémát a pénzváltás. Hátrányai közé sorolható, hogy valamilyen hardver eszközt igényel. A rendszer biztonságát és az anonimitást szolgáltató technikák erősen csökkentik a hatékonyságot, ezáltal költségesebb eszközöket kell alkalmazni, vagy a tranzakciók az elvárható időnél tovább tarthatnak.

A számláló alapú (counter based, register based) rendszerek az egyik legkorábbi digitális pénzrendszerek. Ezeknél egy „számláló” tárolódik a smart card-on. A digitális pénztárcában lévő digitális pénz mennyiségét a számláló által mutatott érték határozza meg. Az általam elemzett érme-alapú rendszerekben a megfelelő információdarabok egy-egy digitális érmét reprezentálnak, melyek előre meghatározott címletűek. A fizetés lényegében ezeknek a digitális érméknek az átadásával valósul meg.

2.1. Digitális pénz sémák

A digitális pénz séma azoknak a protokolloknak, algoritmusoknak és szabályoknak az összessége, melyek segítségével egy digitális pénz funkcionalitású rendszert építhetünk fel.

2.2. A digitális pénz séma szereplői

A digitális vásárlások igényelnek egy vevőt, egy eladót és legalább egy pénzügyi szolgáltató intézményt is. Általában külön intézmény tartozik a vásárlóhoz és az eladóhoz. Alapvető szereplők:

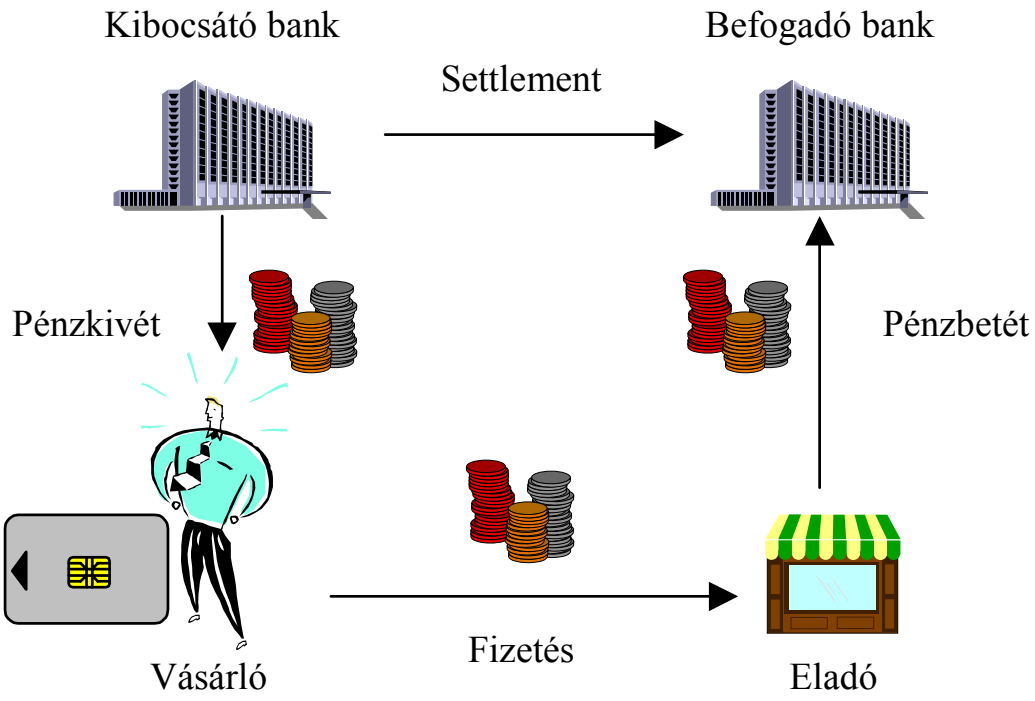
- vevő, vásárló, felhasználó (buyer, payer, user, customer, client);
- kereskedő, bolt, eladó (merchant, payee, shop, seller);
- vásárló bankja, kiadó bank (buyer's bank, issuer bank): a vásárlóval együttműködve digitális pénzt képes kibocsátani;
- kereskedő bankja (merchant's bank, acquirer): a kereskedő mögött álló bank.

Ezen felül fontos szereplők még:

- megbízható harmadik fél (TTP (Trusted Third Party), trustee, ombudsman): a visszavonható anonimitású rendszerben jelenlévő bankrendszertől független szereplők, melyek egy része kormányzati vagy bírósági irányítás alatt, más részük pedig felhasználói jogvédő szervezetek kezében van. Bírói határozat esetén csak az ő együttes segítségükkel lehetséges az anonimitás visszavonása;
- tanúsítvány-kiállító hatóságok (CA, Certification Authority): mivel a rendszerek többsége digitális aláírást használ, ezért szükség van tanúsítvány-kiállító hatóságokra (hitelesítés-szolgáltatókra), illetve a PKI-t (Public Key Infrastructure) felépítő más szervezetek szolgáltatásaira is.

2.3. Egy sémában lezajló főbb fázisok, protokollok

- Pénzkivét fázis (Withdrawal): A felhasználó bankszámlájáról pénzösszeg emelődik le, és digitális pénz formájában belekerül a pénztárcájába.
- Fizetési fázis (Payment): A vásárló a kívánt áruért vagy szolgáltatásért cserébe átadja a kereskedőnek a megfelelő mennyiségű digitális pénzt. A rendszer on-line, ha ebben a fázisban szükséges a bankkal való kommunikáció.
- Pénzbetét fázis (Deposit): A kereskedő a felhasználóktól kapott pénzt beváltja a bankjában, az ezzel egyenértékű összeg megjelenik a bankszámláján.



1. ábra: A digitális pénz áramlása a pénzrendszerben

- Inicializáció fázis (Initialization): a rendszer alapállapotba hozásához és beindításához szükséges műveletek összessége. A banknál az üzemeltetéshez szükséges adatbázisok elindításán és alapvető operációkon kívül a hatékonyság növelése érdekében magába foglalhat különféle előfeldolgozási (preprocessing) műveleteket, inicializáló kommunikációt a trustee entitásokkal.
- Regisztrációs fázis (Registration): Azoknak a műveleteknek az összessége, melyek ahhoz szükségesek, hogy a felhasználó később vásárolhasson a rendszerben. Bekerül a vásárló a banki adatbázisokba, a megfelelő algoritmusokkal kiszámítják a részvételéhez szükséges információkat. Ezek egy része a digitális pénztárcájába kerül. Itt is történhetnek előfeldolgozási lépések (preprocessing) a későbbi hatékonyság növelése érdekében: például az érmék generálásához szükséges adatok egy részének előre kiszámítása. Szükség lehet a trustee szereplőkkel való kommunikációra.
- Nyomkövetés (Tracing): Visszavonható anonimitású rendszerben hatósági utasításra kezdeményezett művelet, melynek során pénzeket, felhasználókat vagy tranzakciókat követnek nyomon. Több fajtáját különböztethetjük meg aszerint, hogy az érmét vagy a tulajdonosát követik vissza, illetve ezenkívül más tulajdonságokat is alapul vesznek.

Osztható pénz esetén bizonyos típusú oszthatóságnál külön fázis jelenhet meg ehhez a tranzakcióhoz tartozóan. Átadható pénznél külön fázis lehet a digitális pénz átruházása, ha az nem a fizetési fázissal egyező protokoll. Külön fázisban jelenhet meg a vitás esetek lekezelése is. Elvesztés-álló pénzeknél szükség van visszakövetelésből és elhelyezésből álló, a pénz visszanyeréséhez tartozó protokollokra.

3. A digitális pénz sémák fejlődése

Az általam vizsgált sémák története az 1980-as évek elejére nyúlik vissza. Ekkor jelentek meg David Chaum alapvető művei, amelyek katalizálták az anonim digitális pénz sémák kutatását. Ötletei és rendszerei alapvető jelentőségűek még ma is, de kutatási aktivitása később sem hagyott alább. Ő találta fel a vak aláírást, és ő alkotott először ennek segítségével feltétel nélküli anonimitást biztosító sémákat. Az ő nevéhez fűződik az egyetlen, a korábbi probálkozásokhoz képest jóval erősebb anonimitást biztosító digitális pénzrendszer, ami meg is valósult, és a gyakorlatban működött. Ez az e-cash elnevezésű on-line rendszer, ami mögött a DigiCash cég állt. Később is döntő fontosságú kutatásokban vett részt Chaum, mint például az off-line sémák kutatása, vagy ehhez a területekhez tartozó kriptográfiai és matematikai primitívek kutatása. Nagy hatással volt tanítványaira is, közülük sokan folytatták a tevékenységüket ugyanezen a területen, és segítették a

tudásukkal, kreativitásukkal a haladást egy ideális rendszer felé (például Stefan Brands is Chaum tanítványa volt).

Először a minél jobb anonimitást biztosító, elsősorban on-line rendszerekre koncentráltak a kutatók, és kidolgozták az ehhez szükséges technikákat. Az anonim on-line rendszerek után szembesültek az anonim off-line rendszerek tervezésénél jelentkező nehézségekkel. Később, az 1990-es évek közepe felé megfogalmazódott a fair off-line digitális pénzrendszerek igénye, amire szintén sok megoldás született. Mindezekkel párhuzamosan állandó célként merül fel a publikált rendszerek hatékonyságának növelése, az anonimitási és biztonsági tulajdonságok kriptográfiailag és komplexitás-elméletileg robosztusabb alapokra való helyezése, a teljes rendszer szigorúbb biztonsági feltételek melletti bizonyítása is.

3.1. Törekvés a privacy elérésére

Kezdetben sok próbálkozás született a privacy elérésére, közelebbről a digitális pénzrendszereket használók magánéletének védelmére, illetőleg személyes adataik védelmére, azonban ez korántsem könnyű. Tekintsük példaként a Mondex rendszert, amelyben minden eszközön van egy kulcspár, a fizetés ezek segítségével történik. A rendszer üzemeltetői azt állítják (nem ellenőrizhető, hogy valóban igaz-e), hogy a TRD-ket (Tamper Resistant Device) olyan elosztási eljárás segítségével adják a tulajdonosaiknak, hogy a bank nem tudja, hogy melyik eszközön melyik kulcspár van.

Az ily módon ajánlott privacy-vel több probléma is van:

1. Nehéz egy ilyen elosztási eljárást megvalósítani, a privacy érdekében bíznunk kell a kiadó cégben/bankban.
2. Az eszközzel elvégzett fizetések linkelhetők lesznek egymáshoz, ugyanis a bank azt azért tudja, hogy melyik eszközhöz melyik kulcspár tartozik (csak azt nem, hogy melyik kártya melyik felhasználóhoz). Ha valamely tranzakció során a felhasználónak azonosítania kell magát, és ily módon kiderül, hogy melyik kártya tartozik hozzá, akkor nemcsak a jövőbeli, hanem az összes múltbeli fizetésének anonimitása is elveszik.
3. A bank biztonsága is gyengébb. Egy eszközt sikeresen feltörő támadó a kulcspárt több fizetésre is képes felhasználni. Pont az eszközterjesztési algoritmus miatt, amely az anonimitást biztosítja, elméletileg lehetetlen a személyazonosságát kitalálni.

Hasonló problémák állnak fenn azoknál a rendszereknél is, amelyek anonim account-ok segítségével biztosítják a privacy-t.

Chaum ismerte fel először, hogy a legkielégítőbb módja a privacy biztosításának az, ha a tanúsítvány kiadásakor a bank által látott információ és a fizetési protokoll során a boltnak adott információ közötti kapcsolat megsemmisül [Cha83]. Mivel annak nincs értelme, hogy a bank tegye meg ezt, ezért magának a felhasználónak kell képesnek lennie erre. Ily módon a felhasználók saját maguk garantálhatják a privacy-t, anélkül, hogy másban meg kellene bízniuk. A gyakorlatban ez azt is jelenti, hogy a digitális érmét a készpénzzel ellentétben a felhasználó állítja elő, a bank csak hitelesíti.

3.2. Vak aláírás alapú sémák, vak aláírás protokoll (blind signature protocol)

A vak aláírás protokollhoz a következő fizikai analógia képzelhető el. Az aláírás fogadó belehelyezi az aláírandó dokumentumot egy indigós papírral együtt egy borítékba, majd lezárja a borítékot. Az aláíró aláírja a borítékot anélkül, hogy kinyitná azt, vagy bármely módon tudomást szerezne a tartalmáról. A fogadó ezután megkapja a borítékot, melyben a dokumentum már alá van írva. A hitelességet a fogadó bárkinek bizonyítani is tudja az aláírás felmutatásával.

A vak aláírás egy két-résztvevős protokoll, jelen esetben a *V* vásárló és a kibocsátó *B* bank között. A protokoll célja, hogy *V* aláírást szerezzen *B*-től egy *M*-re úgy, hogy *B* ne tudjon meg semmit *M*-ről. A *V* ehhez először választ egy *R* „vakolási”[1] faktort (blinding factor), ami egy véletlen szám, illetve egy *F(,)* egyirányú „vakoló” függvényt, amely olyan, hogy minden *M*-re bármely *R* esetén *F(M,R)* egyenletes eloszlású az üzenet tér felett. *V F(,)* segítségével kiszámolja $M' = F(M,R)$-t, és megkéri *B*-t, hogy generáljon $SIG_{SK\_B}(M')$ aláírást az *M'*-re. Ezután a *V* a *G(,)* „kivakoló” függvényt használja, hogy kiszámolja $SIG_{SK\_B}(M) = G(SIG_{SK\_B}(M'),R)$-t.

[1] *A szerkesztő megjegyzése:* Az eredeti, „blind signature” (vak aláírás) kifejezésből származtatott további fogalmak szó szerinti fordítása magyarul rosszul hangzó, sőt értelmetlen képzeteket keltő kifejezéseket eredményez. A „blinded digital coin” például megvakított digitális érme lenne. A magyar szakirodalomban javasolt egyik megoldás — éppen az említett fizikai analógiára utalva — a *„borítékolt digitális bankó”,* tehát a „blinding” a borítékolás kifejezéssel, a „digital coin” a digitális bankó kifejezéssel jelölhető, lásd [Szé00]. Ennek alapján a „blinding factor” *borítékoló faktornak* fordítható, hasonlóképpen beszélhetünk „borítékoló” és „borítékbontó” függvényről.
A szerző sajátos megoldást választott a „blinding” és a kapcsolódó fogalmak magyarítására: a két szó hangalakjának hasonlóságát kihasználva a „vakítást” „vakolás”-nak fordítja, utalva egyúttal a vakolás elfedő, elrejtő funkciójára. Ebből következően beszél „bevakoló” és „kivakoló” függvényről, „vakolási” faktorról, „vakolt” aláírásról. A nyelvi leleményt elismerve, egyúttal az egységes magyar szóhasználat hiányát figyelembe véve megtartottuk ezt a szóhasználatot, azonban mindenütt idézőjelbe téve, hogy elkerüljük téves értelmezését.

A digitális pénzrendszerekben ilyen protokollt az érme-generáláshoz használnak. Az *M* aláírandó üzenet tulajdonképpen a pénzérme. Látható, hogy ezt a vásárló állítja elő, így megőrződhet anonimitása. Mikor a kereskedő beváltja *M*-et, akkor a banknak fogalma sem lesz arról, hogy ki számára bocsátotta azt ki, hiszen az *M′* eloszlása teljesen független *M*-től.

F(,) tulajdonságai miatt, és mivel az *R* véletlen, csak a Vásárló által ismert, ezért a Banknak nincs tudomása arról, hogy mit írt alá. Ennek ellenére mindenki, aki ismeri a Bank nyilvános kulcsát, meg tud bizonyosodni róla, hogy az aláírás hiteles.

A „vakolásnak" több fajtáját lehet megkülönböztetni [FY94]:

- „vakolt" ellenőrzéses aláírás: megakadályozza az aláírót abban, hogy későbbiekben felismerje magát az aláírást, miközben nem szükségszerűen rejti el az aláírandó üzenetet.
- „vakolt" üzenetes aláírás: megakadályozza az aláírót abban, hogy későbbiekben felismerje magát az üzenetet, miközben nem szükségszerűen rejti el az aláírást.
- teljesen „vakolt" aláírás: az előbbi két tulajdonság együttes teljesülése egy sémában (az eredeti Chaum értelemben vett vak aláírás)

A legtöbb tárgyalt aláírás teljes vak aláírás. A vak aláírás önmagában csak a nyomkövethetetlenséget biztosítja, nem véd a túlköltések ellen. Csak az úgynevezett one-show típusú vak aláírások [CFN90] garantálják, hogy akkor és csak akkor fedődik fel a tulajdonos kiléte, ha többször próbálja elkölteni ugyanazt a pénzt.

A digitális pénzrendszerben nem kívánatos, ha a vásárlónak bármilyen *M* érték választását megengedjük. A sémák igényelik, hogy az érme adott formátumú legyen, és bizonyos információkat tartalmazzon, mint például az érme címlete. On-line és off-line sémákban egyaránt meg kell győződnie a banknak, hogy az általa nem látott érme teljesíti az érvényességhez szükséges követelményeket (helyes a formátum, a vásárló az identitását megfelelően kódolja, stb.). Ennek érdekében a vak aláírásokat cut-and-choose (3.6. fejezet) ellenőrzéssel, vagy zero-knowledge proof-fal (3.4. fejezet) kombinálják.

Az első ilyen off-line séma, a Chaum-Fiat-Naor [CFN90] cut-and-choose paradigmát (3.6. fejezet) használ, és RSA rejtjelezésen alapul. Heurisztikus a megközelítés, a biztonságra nincs teljes bizonyítás, később biztonsági réseket is találtak a rendszerben. A cut-and-choose megközelítés óriási érme-méretekhez vezet, nagy számítási teljesítményt igényel, nem hatékony.

A vak aláírások olyan implementációja is lehetséges, ahol több résztvevő is egyszerre részt vesz a számításban. A számításhoz a bank szolgáltatja az egyik bemenetet (titkos aláíró kulcs), a vásárló a másikat (aláírandó üzenet), és végül egyedül a vásárló kapja meg a kimenetet (aláírt üzenet). A biztonság alapvető kriptográfiai feltételezésekre visszavezethető. Azonban az ilyen több-résztvevős protokollok hatékony megvalósítása nagy kihívást jelent (3.15. fejezet).

3.2.1. Vak RSA aláírás

Konkrét példaként nézzük meg a [Cha83] által bemutatott RSA-n alapuló vak aláírást. Legyen a Bank RSA kulcsához tartozóan $N = PQ$ egy nyilvános RSA modulus, d és e a titkos és a nyilvános kitevők. A vak aláírás kiszámolásához V generál egy $R \bmod N$ véletlen számot, és kiszámolja $M' = F(M,R) = R^eM$-et. Ezután B kiszámol rá egy aláírást $(R^eM)^d = RM^d$. V az M^d-t megkapja, ha elosztja RM^d-t $R \bmod N$-el (azaz $G(K,R) = K/R \bmod N$). Természetesen mivel RSA aláírásról van szó, minden művelet $\bmod N$ értendő. Vegyük észre, hogy konkrét példában fontos szerepe van annak, hogy az RSA kommutatív (felcserélhető végrehajtási sorrendű) aláírási és szorzási operációkkal rendelkező séma.

Az RSA aláírással vigyázni kell, mert ahogy Goldwasser, Micali és Rivest rámutatott, önmagukban még nem állják ki az adaptive choosen plaintext típusú támadást. Először is, mivel a nyilvános kulcs ismert, mindig lehetséges hamisítani egy „véletlen” tartalmú üzenethez egy aláírást. Másodszor pedig, az RSA művelet multiplikatív homomorf tulajdonsága miatt az üzenetek mindenfajta inverziója, transzformáltja és ezek szorzata hamisítható, ha az eredeti üzenet aláírása ismert.

Azonban ha egy alkalmas egyirányú $h()$ hash függvényt használnak az üzenet keverésére az RSA operáció előtt, akkor ezek a támadások meghiúsulnak, ezt használta ki Chaum és Evertse, és részleteiben tárgyalja Damgard. A $h()$ függvény befolyásolja az üzenet-teret a multiplikatív homomorfizmuson alapuló támadások megakadályozása végett, miközben megőrzi az RSA homomorfizmusát, így vak aláírások kivitelezése is lehetséges.

Számos gyakorlatban előforduló hiba is veszélyeztetheti a rendszer erősségét, mint például egymáshoz közel álló prímpár választása. Másik gyakori hiba a viszonylag kicsi, és 2^k-1 alakú nyilvános kitevő választása, ami ugyan praktikusnak tűnik, mert felgyorsítja a számításokat, azonban kiderült, hogy csökkenti a rendszer biztonságát.

3.2.2. Vak Schnorr aláírás

3.2.2.1. Schnorr azonosítási séma

A Schnorr aláírás séma a Schnorr azonosítási sémán alapul (Schnorr identification scheme) [Bra95a] [Sch91]. A Schnorr sémákban minden aritmetikai művelet az olyan q prím rendű G_q csoportban zajlik, mely esetében polinom idejű algoritmusok ismertek a szorzásra, egyenlőség vizsgálatra, csoporttagság vizsgálatra, és véletlenszerű elemválasztásra, de nem ismert olyan algoritmus, ami a G_q alapú diszkrét logaritmus számítására kivitelezhető. Az irodalomban már elég sok ilyen tulajdonságú csoport ismert.

A protokollban a két résztvevő fél a V ellenőrző (Verifier) és a P bizonyító (Prover). A kulcsgenerálási algoritmus a Schnorr azonosítási sémához a k bemeneti paraméterhez generál egy (q,g,h) nyilvános kulcsot, és egy hozzá tartozó $\lg_g h$ titkos kulcsot a PPT bizonyító P számára.

P bebizonyíthatja a titkos kulcs ismeretét egy PPT V ellenőrzőnek a Schnorr azonosítási sémában definiált kihívás-válasz alapú azonosítási protokollal. Schnorr megmutatta, hogy ez a protokoll egy tudásbizonyítéknak (proof of knowledge) is megfeleltethető, ha V a kihívást egyenletes valószínűségi, vagy ahhoz közeli eloszlással generálja. Azonban a protokoll feltételezhetően nem zero-knowledge: általánosságban csak szemtanú elrejtő (witness hiding) protokollnak vélik.

3.2.2.1. Vak Schnorr aláírási séma

Fiattól és Shamirtól származik egy általános technika, aminek alkalmazásával a tudásbizonyítási protokollt aláírás-kiadási protokollá lehet konvertálni. Ez a Schnorr azonosítási sémára is megtehető. Implicit módon a kulcsgenerálási algoritmus is megváltozik.

Az interakció eltávolítható az új protokollból, mert a c kihívást maga a P is meghatározhatja. Az interakció kiküszöbölésével V egy olyan m üzenet számára szerezhet aláírást, mely P előtt nem ismert. Sőt, ahogy Ohta és Okamoto megmutatta, V ezen felül „vakolhatja” a (c,r) aláírást. Megmutatható, hogy az eredményül kapott összetartozó (üzenet, Schnorr aláírás) párok, az aláírás-kiadási protokoll végrehajtása során P által látottakhoz nem korrelálnak. Más szavakkal, ez a protokoll egy vak aláírás kibocsátási protokoll, ahogyan a [Cha83]-ban informálisan definiálva van.

A végső protokollt hívják vak Schnorr aláírás kiadási protokollnak. A kulcsgenerálási algoritmust, az aláíró és ellenőrző protokollt együttesen Schnorr aláírási sémának nevezzük.

3.3. Zero-knowledge technikák

A zero-knowledge protokollok során a résztvevő felek úgy szerepelnek a protokollban, hogy közben az egyik fél előtt a másik fél bizonyos információi rejtve maradnak (nem tud meg semmit róluk), pedig a protokoll végeredményében szerves része van ennek a titoknak is. Gyakran explicit is megjelenik a protokollok során a zero-knowledge bizonyíték (zero-knowledge proof). Ez egy olyan bizonyítékul szolgáló információ, amelynek segítségével egy bizonyító meg tud győzni egy ellenőrző felet arról, hogy ismer egy x titkot, miközben x-ről semmiféle információt sem fed fel.

Az on-line, feltétel-nélküli anonimitású rendszerek időszaka után hatékony off-line rendszereket próbáltak kifejleszteni a kutatók. Off-line esetben a kereskedő a digitális pénz hiteleségét a bankkal való kapcsolatteremtés nélkül ellenőrizheti le. Igen előnyös tulajdonság az off-line fizetés, de ára van: nem lehet az elkövetésének pillanatában megakadályozni a dupla költést, vagyis hogy egy rosszindulatú felhasználó többször költsön el egy elektronikus érmét (hacsak nem tételezünk fel a rendszerben manipulálás-védett eszközt, rajta egy megfigyelővel, aki betartatja a szabályokat). A védekezés úgy valósul meg, hogy ha dupla költés fordul elő, akkor bizonyos idő elteltével garantáltan detektálódik, és a rosszindulatú felhasználó anonimitása megszűnik, kiderül a személyazonossága.

Követelmény a dupla költés detektálásán kívül, hogy a pénz hamisíthatatlan, újrafelhasználhatatlan, nyomkövethetetlen legyen. A séma lehetőleg off-line legyen, azaz a vásárlási protokollban ne vegyen részt a bank, mint ahogy ez a hagyományos készpénz esetén is igaz. Hogy az anonimitás teljesüljön, de a túlköltés is érzékelhető legyen, minden pénzérmébe bele kell foglalni láthatatlan módon a vásárló kilétét úgy, hogy az csak és kizárólag többszöri elköltés esetén derülhessen ki. Ezenkívül, hogy a vásárló privacy követelménye és a bank hamisítás elleni kívánalma is egyensúlyban legyen, minden érmét hitelesítenie kell a banknak, anélkül, hogy látná azt. E követelményeket egyszerre kielégíteni nagyon nehéz feladat, több megoldás is született rá, melyeket a későbbiekben részletesebben is szemügyre veszek.

Azért, hogy a komplex elvárásokból fakadó összetett tulajdonságokat és biztonsági feltételeket mind kielégíthessük, a digitális pénzrendszerek zero-knowledge számításokat használnak a séma több fázisában.

Tekintsünk egy hagyományosnak mondható digitális pénz sémát. A digitális érme egy vak aláírással, vagy ezzel ekvivalens protokollal hitelesítődik a bank részéről, tehát a bank nem látja sem az éppen kibocsátott pénzérmét, sem a konkrét aláírást. Az aláírás segítségével a boltos egyértelműen megbizonyosodhat arról, hogy a pénz valódi. A dupla költés elleni védelem érdekében az elektronikus érmének titokként beágyazva tartalmaznia kell a felhasználó identitását, mégpedig úgy, hogy az csak és kizárólag dupla költés esetén derülhessen ki. Természetesen, mielőtt a bank aláír egy érmét, meg kell győződnie, hogy a titok-beágyazás az előírások szerint történt. Itt kap megint nagyon fontos szerepet a zero-knowledge technika: a bank ennek segítségével le tudja ellenőrizni az érme struktúráját anélkül, hogy bármilyen részletet vagy információt megtudna róla, vagy az anonimitást megsértené.

A zero-knowledge, illetve a vak aláírás a legköltségesebb protokollok az elektronikus érme generálás során. A digitális pénzrendszerek szűk keresztmetszetét jelentik számítási és kommunikációs oldalról is. Bizonyíthatóságuk és biztonságuk a teljes rendszer ugyanezen tulajdonságainak alappillérei, így rendkívüli fontossággal bírnak.

3.4. Zero-knowledge proofs of knowledge-en alapuló rendszerek

A zero-knowledge proof of knowledge — Goldwasser, Micali és Rackoff alapján — egy olyan protokoll, amely egy bizonyító fél (prover) és egy ellenőrző fél (verifier) közötti kommunikációt határoz meg, melynek során az ellenőrző anélkül győződik meg arról, hogy a bizonyító birtokában van egy bizonyítéknak (bizonyságnak), hogy közben bármit is megtudna magáról a bizonyítékról. DeSantis és Persiano megmutatta, hogy ha lehetséges zero-knowledge proofs of knowledge-ek használata, akkor nem feltétlenül szükségesek vak aláírások az off-line sémához.

Az alapötlet az, hogy a bank küld egy aláírást a vevőnek, de soha nem látja ezt az aláírást többé senki. Ahelyett, hogy magát az aláírást mutatnánk be vásárláskor az érme érvényességének igazolására, a vásárló egy bizonyítékot mutat be az eladónak arról, hogy az ő birtokában van egy érvényes aláírás a banktól. Az érme beváltáshoz az eladó bemutat egy bizonyítékot arról, hogy egy érvényes bizonyítéka van arról, hogy a vásárlójának egy érvényes bizonyítéka van.

Az ilyen típusú sémák biztonsága is visszavezethető alapvető kriptográfiai feltételezésekre. Mindazonáltal az üzenetek és a rejtjelezések komplexitása meglehetősen nagy lehet.

3.5. Felejtő hitelesítés (oblivious authentication)

A felejtő hitelesítés egy kriptográfiai protokoll primitív, ami során egy azonosító hatóság (authorizing agency) egy szemtanúval (witness, a beágyazott titok tanúja) együtt egy beágyazott titokkal rendelkező útlevelet (passport = hitelesített dokumentum egy megbízható forrástól, ami azonosítja a tulajdonosát) bocsát ki. A kiadási procedúra olyan értelemben feledékeny, hogy a kiadóhivatal a kiadás után már nem tudja egyik útlevelet se összefüggésbe hozni a kiadási időponttal. Az útlevél szemtanú nélküli használata sorozatos hitelesítést tesz lehetővé, a titok rejtve marad. Az útlevél tanúval együtt való használata azonosítaná a felhasználót és felfedné a beágyazott titkot, ezért az útlevelet a szemtanú „utalás"-ával („hint"-jével) együtt használják, ahol bármely két hint elegendő a szemtanú felfedéséhez, de egy „hint" sohasem. Vegyük észre, hogyha a beágyazott titok a felhasználó kiléte, akkor pont megoldhatjuk egy off-line érme és a hozzá tartozó séma készítésének problémáját.

[FY93]-ban a pénzkivét protokoll a felejtő hitelesítésnek egy olyan példánya, ahol a bank ad ki egy útlevelet a felhasználó identitásának beágyazásával, és a vásárló számára egy tanúval. A vásárlás elvégzéséhez a vásárló odaadja az eladónak az útlevelet és egy egyedi utalást (amit a szemtanúból állít elő). A pénzbetét tranzakcióhoz az eladó továbbítja az útlevelet és az utalást a banknak.

Az bebizonyítható, hogy ily módon egy biztonságos off-line pénzérme séma alkotható bármely felejtő hitelesítés séma használatával. Konkrétabban, az [FY93] új felejtő hitelesítés sémája a [FY93] új beágyazott sémájával együtt egy bizonyíthatóan biztonságos és hatékony off-line pénz sémát eredményez. A beágyazó séma célja, hogy elrejtsen egy titkot olymódon, hogy az a szemtanú nélkül rejtve maradjon. Ezen kívül lehetővé kell tennie ellenőrizhető utalások előállítását (amelyek közül bármely kettő felfedi a titkot). A séma biztonsága a DLP komplexitásán nyugszik. Ez az első single-term megközelítés, ami sokkal kompaktabb, mint a híres cut-and-choose technika.

A [FY93] a felejtő hitelesítést előfeldolgozási lépéssel segített egyirányú hash függvényekkel oldja meg. Az előfeldolgozási lépés megbízott ágenseken alapulhat, melyek jelen vannak az inicializálásnál, és el vannak választva a banktól, az eladóktól és a vevőktől. Ezek az ágensek, amelyeket trusted manufacturer-nek is hívnak, feltölthetik felhasználók smart card-jainak memóriáját sok string-gel, majd saját maguknál megsemmisítik az ezek generálásával kapcsolatos adatokat. A smart card memóriájának nem kell védettnek lennie, az egyetlen követelmény, hogy a megbízott ágens megfelelő formátumú stringekkel töltse fel, és ne adjon ugyanolyan stringet senkinek. Ez az ártatlan

feltételezés sajnos az off-line pénzrendszer biztonságosságának kérdését nagyon megnehezíti.

A pre-processing fázis végrehajtható ágensek nélkül is, de ekkor nem hatékony, magas rangú polinom kommunikáció szükséges a bank és a vevő között (lényegében egy cut-and-choose alapú protokoll). A pénzkivét, vásárlás és pénzbetét protokollok hatékonysága változatlan marad ekkor. A pre-processing protokollnak az Even, Goldreich és Micali-féle „on-line/off-line" aláírás sémához nagyon hasonló realizációja képzelhető el. Csak akkor single-term a rendszer, ha a gyenge feltételezést elfogadjuk, és ágenseket engedünk használni.

3.6. Megfelelő formátumú érvényes érme előállítása, Cut-and-choose protokoll

Az anonimitáshoz szükséges a vak aláírás technika alkalmazása, azonban valamilyen módszerrel lehetővé kell tenni, hogy csalás esetén (tipikusan dupla költés) a vásárló kiléte kiderüljön. A cut-and-choose protokoll egy módszer arra, hogy olyan érméket generálhassunk, amelyek megfelelő struktúrával rendelkeznek, amelyek hordozzák az ehhez szükséges információkat, de mégis megőrizzék a vak aláírások által az ügyfél számára biztosított anonimitást. A módszert számos korai rendszerben használják [Cha90] [Oka92] [Sch96].

A klasszikus megközelítés szerint az ügyfél érme-kivételkor generál n darab megfelelő formátumú érmét, „vakolja" őket különböző „vakolási" faktorral a vak aláírásnál leírtak szerint, és elküldi ezeket a banknak. A bank véletlenszerűen kiválaszt ezek közül n-1 darabot, és megkéri az ügyfelet, hogy mutassa fel az ezekhez tartozó „vakolási" faktorokat.[2] A bank „kivakolja" ezek segítségével a választott érméket, és meggyőződik róla, hogy azok megfelelő formátumúak. Ezek után aláírja az egyetlen „kivakolatlan" érmét, és visszaadja az ügyfélnek.

1 az n-hez az esélye, hogy a bank helytelen formátumú érmét ír alá. Feltételezhető, hogy a csalás megkísérlésének büntetése elég nagy ahhoz, hogy senki se kockáztassa meg a megúszásnak az 1/n-es esélyét.

A módszer rengeteg felesleges (később fel nem használt) érme generálását és elküldését igényli ahhoz, hogy egy érvényes érmét eredményezzen. Ez sok számítási és kommunikációs költséget jelent, főleg, hogy az érmében általában valamilyen módon

[2] Egy rosszindulatú felhasználó nyilvánvalóan nem adná ki a kezéből azt a „vakolási" faktort, amely alapján később felelősségre vonható lenne, inkább megszakítaná a tranzakciót — *a szerkesztő megjegyzése.*

rejtjelezett illetve hitelesített információkat kell elhelyezni. Sajnos a csalás valószínűségének csökkenésével (n növelése) arányosan nőnek ezek a költségek is. A cut-and-choose paradigma nem csak a hagyományos vak aláírásokkal együtt alkalmazható, hanem más technikákkal kombinálva is; az más kérdés, hogy érdemesebb kevésbé költséges megoldást használni.

3.7. Off-line rendszerek

Az off-line digitális pénzrendszerekbe az anonimitás beépítése még nehezebb dolognak bizonyult, mint az on-line rendszereknél [Bra93]. Ugyanazt a biztonságot kell nyújtani, mint on-line esetben, így például a duplán elköltés ellen is valamilyen védelem szükséges. Off-line megoldás esetén azonban nincs lehetőségünk a bankkal kapcsolatot teremteni, hogy segítsen. Két fő koncepció kínálkozik.

Az egyik lehetőség az on-line rendszereknél is alkalmazott one-show vak aláírás vagy ezzel egyenértékű módszer használata. A probléma ott van, hogy ezekkel az eset megtörténtének pillanatában nem fedhetők fel a duplán költések, csak a csalás után bizonyos idővel (after the fact). Mégpedig abban a pillanatban, amikor egy becsapott boltos a második érmével fordul a bankhoz, és a speciális tulajdonság miatt egynél több rendelkezésre álló aláírásból (az érme része) az elkövető kiléte kiderül.

A második koncepció szerint a felhasználó elektronikus pénztárcájába gyárilag egy megfigyelő van beágyazva (wallets with observers), aki a csalást még az elkövetése előtt meg tudja akadályozni. Ez szintén nem egyszerű megoldás, hiszen a smart card-ok vagy a PDA-k (melyek valószínűleg elektronikus pénztárcák lesznek majd) mind számítási, mind tárolási kapacitásban igen korlátozottak. Tehát a megfigyelő működésének és protokolljainak nagyon hatékonynak kell lennie. Egy probléma, hogy a megfigyelő csak akkor képes a feladatát végrehajtani, ha biztosítják a sértetlenségét, védik a manipulálás ellen. A smart card-ot sokszor sérthetetlen eszköznek tételezik fel (Tamper Resistent Device, azaz manipulálás-védett eszköz), azonban ez nem bizonyított, és több példa is volt már arra, hogy valamilyen törhetőséget publikáltak (például teljesítményfelvétel-elemzéses támadás). Azok a rendszerek, amelyek törhetetlenségének egyik feltétele az elektronikus pénztárca sérthetetlensége, sajnos biztonsági szempontból nem kielégítők. Éppen ezért a megfigyelővel is rendelkező sémákat úgy kell megtervezni, hogy egy előző esetbe sorolandó séma képezze az alapját. Vagyis ha esetleg kiiktatják a megfigyelőt, akkor a csalások érzékelése az első koncepció szerinti mechanizmusokkal még mindig lehetséges, a de-anonimizáló eljárások mindig bevethetők maradnak.

A fenti gondolat már a fair fizetési rendszerek megjelenése előtt is megfogalmazódott [Bra93], de ugyanúgy érvényes ezekre a sémákra is. Vagyis a TTP (Trusted Third Party) részvételével nyomkövethető elektronikus protokollok biztonságát szintén hiba lenne részben vagy egészben az elektronikus tárca sérthetetlenségére alapozni. Ilyenkor a rendszer alapját egy megfelelő fair off-line pénz sémának kell alkotnia, és sikeres manipulálás esetén az alap nyomkövetési eljárások még mindig rendelkezésre állnak a csalás felderítésére.

A fent vázoltak alapján a publikált rendszerek általában két csoportra oszlanak. Az első csoportba tartozó sémák alapkutatáshoz tartoznak. Általában vagy új megoldást mutatnak be, vagy egy létező megoldást fejlesztenek tovább. Nem kész rendszerek, bár a tervezésüknél fontos irányelv volt az implementálhatóság. A második csoportba tartozó rendszerek valamelyik előbb említett sémán alapulnak, kiegészítik azt második típusú rendszerré, miközben ehhez esetleg az alapsémában is kisebb-nagyobb módosításokra van szükség.

3.8. Wallets-with-observers paradigma

A korábban említett második koncepció, amely a dupla költés előzetes megakadályozását kínálja, szintén megvalósítható privacy-védő esetben is. Itt a felhasználó egy fizetőeszközzel rendelkezik (például PDA, smart card). Ennek egy részébe be van ágyazva egy ún. megfigyelő (observer), ami egy speciális sérthetetlen részen (TRD) helyezkedik el, ez akadályozza meg előzetesen az érmék dupla elköltését. A beágyazásnak oly módon kell történnie, hogy minden üzenet, amely a külvilág felől jön, áthaladjon a megfigyelőn és fizetőeszközön is, illetve minden üzenet, ami akármelyiküktől származik és a külvilág felé megy, keresztülmenjen mindkét eszközön. Ez egyrészt lehetővé teszi a megfigyelő számára, hogy kifejtse a védelmi tevékenységét. Egy fizetés csak akkor valósulhat meg, ha a megfigyelő is együttműködik. A felhasználó számára pedig lehetővé teszi, hogy felismerje, ha esetlegesen a megfigyelő de-anonimizálási vagy egyéb célzattal érzékeny információkat próbál kiszivárogtatni.

Chaum foglalkozott először ehhez nagyon hasonló problémával ([BC90] [Cha92] [CP92]). A korai időkben internetes fizetésekhez tervezett on-line sémákról volt szó. A javasolt felállásban a számlatulajdonos a bank által adott TRD-t csatlakoztatott a számítógépéhez olymódon, hogy az összes külvilág felől vagy külvilág felé áramló információnak mindenképpen keresztül kellett mennie a felhasználó hardverén is.

A beágyazás fent leírt tulajdonsága természetesen kriptográfiai eszközökkel garantált. A bank és az eszköz között elhelyezkedő felhasználó által irányított számítógép olymódon

szabályozhatja a kommunikációt, hogy a „vakolási” protokoll bizonyosan megfelelő módon játszódjon le, és a két fél között rejtett csatornákon ne cserélődhessen ki információ (shared information) a tanúsítványkiadó algoritmus során [Cha92]. Ilyen konfigurációban privacy-t biztosító protokollok tervezése nem is olyan könnyű, hiszen biztonságos két-résztvevős protokollok helyett biztonságos három-résztvevős protokollokra van szükség.

Chaum és Pedersen [CP92] a wallets-with-observer paradigmával foglalkozik. A forrás ezzel kapcsolatban a formális definíciók és a metodológia leírását is tartalmazza. Analizálja és megpróbálja javítani mindenféle értelemben az ilyen konfigurációkban használható protokollokat.

A shared-information fogalmat Cramer és Pedersen [CP93b] használta először: osztott információnak (shared information) nevezzük azt a kölcsönösen ismert információt, amely lehetővé teszi a nyomkövetést. Ez mind bejövő, mind kimenő részt tartalmazhat. Bár feleslegesnek látszik, hogy esetlegesen osztott információ előállításától tartsunk, egyáltalán nem nehéz olyan rendszert készíteni, amely be- és kijövő rész nélkül is megsértheti a privacy-t. Például úgy, ha az observer és a bank a kártya gyártásakor kölcsönösen generálnak egy véletlen számot, amit később a megfigyelő mindig eljuttat fizetéskor a bankhoz.

Fontos gondolat, amit Brands is többször hangsúlyozott, hogy nem szabad a biztonságot csak a TRD-re alapozni. Ha egy számlatulajdonos nem várt módon feltöri a TRD-t és duplán költ, akkor még mindig felderíthetőnek kell maradnia az eset után. Ez azt jelenti, hogy az első koncepció biztonsági hálóként szolgál ilyen esetben, és a második koncepciónak mindenképpen egy első koncepciós rendszer kiterjesztettjének kell lennie. Nem egyszerű probléma ezt megtenni úgy, hogy az alaprendszer biztonsága ne gyengüljön, és a hatékonysága se romoljon. A [Bra93] rendszer hatékony marad, az observer-es számítás kapacitása mindössze Schnorr azonosítási sémák elvégzésének képességét igényli. A Ferguson [Fer94] sémának is javasolnak például ilyen kiterjesztést, azonban ott tovább romlik az alaprendszer biztonságának bizonyíthatósági problémája és a hatékonysága.

3.9. Felhasználói identitás beágyazása az érmébe one-show vak aláírási technikákhoz

Az off-line fizetések lehetősége nagyobb szabadságot biztosít az elektronikus fizetőeszköz használatában. Azonban a digitális adat tökéletesen lemásolható; pusztán egy bitsorozatnak is tekinthető. Dupla költésről beszélünk akkor, ha ugyanazt az érmét két vagy több fizetésnél is használják, és a fizetések összege meghaladja az érme értékét. Nem osztható érmék esetén a fizetés összege az érme címletével megegyezik. Off-line típusú eszköz esetén manipulálás-védett eszköz használata nélkül nincs lehetőség a dupla költés

megakadályozására. Viszont lehetőség van arra, hogy bárkinek, aki duplán költ, a kiléte kiderüljön, így szankcionálhatóvá váljon. A fair felhasználók anonimitásának megőrzése érdekében nem szabad hogy kiderüljön az olyan ügyfelek identitása, akik nem követtek el semmilyen csalást.

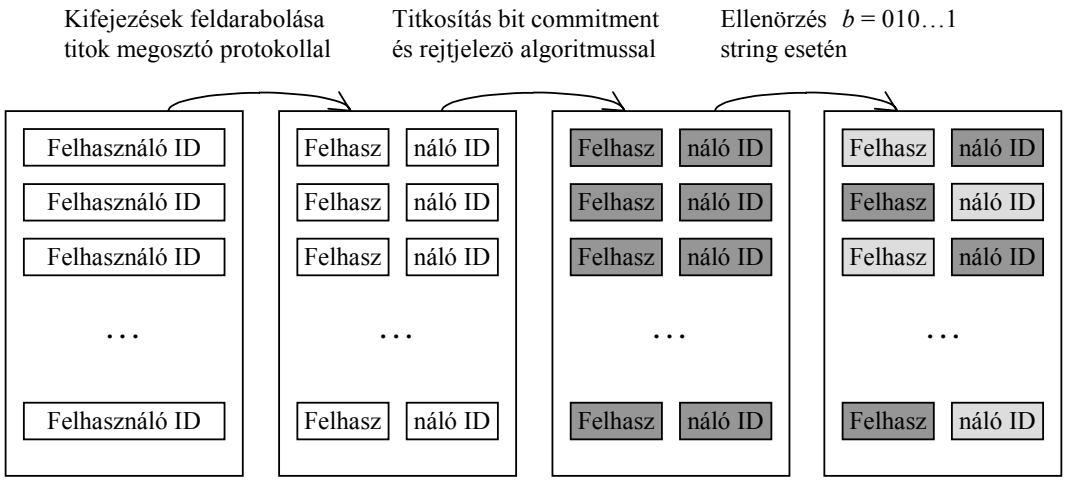
Az anonimitási technikák segítségével kisebb-nagyobb erőfeszítéssel elérték, hogy a felhasználó identitása ne derüljön ki se a pénzkivét fázis, se más fázisok során. A csalás elleni védekezéssel bizonyos szemszögből nézve megfordul a helyzet, az érmébe direkt bele kell raknunk az ügyfél kilétét, de olyan cseles módon, hogy az csak és kizárólag a szükséges esetekben legyen megnézhető.

Erre számos módszer létezik. Mindegyik ilyen sémában a vásárló identitását valamilyen módon belekódolják az érmébe. A fizetési fázis során a vásárló felmutatja az érmében tárolt identitás egy részét, vagy az identitásának egy függvénnyel való transzformáltját. Így, ha a bank két olyan tranzakció adatát kapja meg, melyben ugyanazzal az érmével költekeztek, az érmében tárolt identitás kideríthető.

3.9.1. Multiple-term off-line érmék

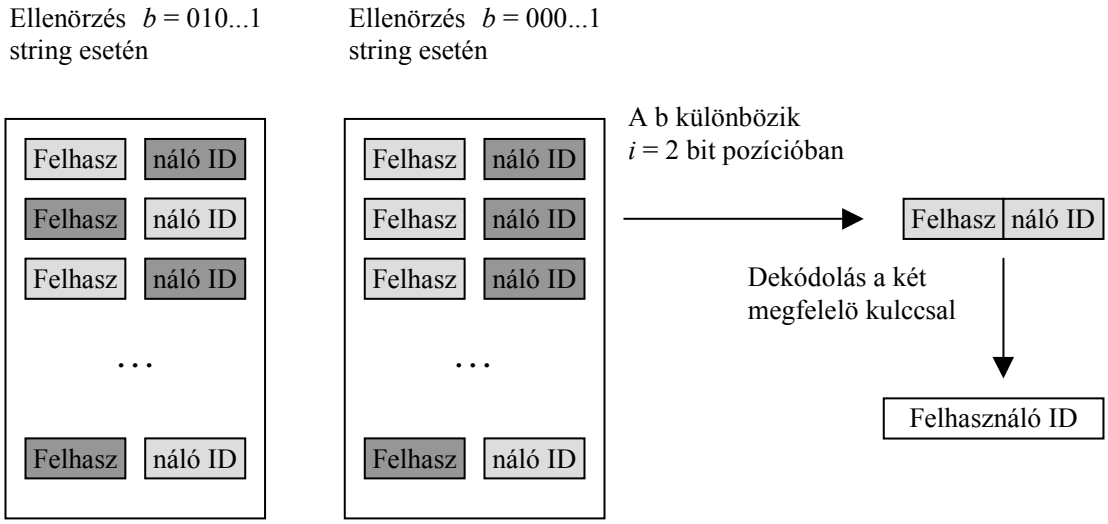
Multiple-term off-line érmét használó sémában az érme n darab kifejezést (term) tárol. Mindegyik kifejezés tartalmazza a pénzt kivevő vásárló azonosító számát (ID). Mindegyik kifejezés egy titokmegosztó protokoll segítségével két részre vágódik szét. A titokmegosztó protokoll olyan, hogy egy fél kifejezés ismerete semmilyen információt nem fed fel a teljes kifejezésből. Viszont két összeillő fél-kifejezésből összeilleszthető a teljes ID-t tároló kifejezés. Az összes $2n$ darab fél, ij, $i = 1, \ldots, n$, $j = 0, 1$, egy bit-kommitment protokollon esik át, ezután pedig rejtjeleződik különböző k_{ij} kulcsokkal. A bit-kommitment protokoll biztosítja, hogy ha egy fél kifejezést kirejtjeleznek, akkor a rejtjelezés helyessége ellenőrizhető.

A fizetési fázis során az üzlet, miután megkapja az érmét és hitelességét leellenőrzi, választ egy n bit hosszúságú véletlen bitfűzért, $b_1, b_2, b_3, \ldots, b_n$, és elküldi a vásárlónak. A vásárló elküldi az ennek megfelelő $k_1b_1, k_2b_2, k_3b_3, \ldots, k_nb_n$ kulcsokat az üzletnek. Az üzlet dekódolja a megfelelő fél-kifejezéseket, és ellenőrzi, hogy azok valóban helyesen lettek-e dekódolva. A pénzbetét fázis során az üzlet elküldi az érmét és a kulcsokat a banknak.



2. ábra: Beágyazás folyamata a multiple-term érméknél

Ha az érmét másodszorra költik el, akkor a fizetési fázis hasonló lépések szerint zajlik azzal a különbséggel, hogy nagy valószínűséggel más véletlen bitfűzért választ az üzlet. Ha csupán egy bit is különbözik — legyen mondjuk ez az *i*-edik —, akkor az *i*-edik kifejezés mindkét felét ki tudja rejtjelezni a bank, szóval az érmét a bankból kivevő felhasználó kiléte kiderül.



3. ábra: Duplaköltés esete a multiple-term érméknél

Elképzelhető persze, hogy egy vásárló és egy üzlet cinkos egy csalásban, és az elfedés érdekében az üzlet ugyanazt a véletlen bitfűzért sorsolja mindkét elköltésnél. Ez nem jelent problémát, ha a bank ilyen esetben (ugyanazt az érmét kétszer költik el ugyanazzal a véletlen bitfüzérrel) csak egyszer adja oda az üzletnek a pénzt. Több cinkos bolt esetén megoldás lehet, hogy a bitfüzér egy darabja előre meghatározott, minden üzletre nézve egyedi.

Nagy probléma a multiple-term off-line érmékkel a kifejezések száma. Ez meglehetősen naggyá teszi az érme méretét, és ezáltal a kommunikációs költségeket is. Ezenkívül természetesen a sok rejtjelezés miatt a számítási költség is arányosan nő.

3.9.2. Single-term off-line érmék

Single-term off-line érmék esetén olyan speciális matematikai elvek alapján konstruálják meg az érmébe helyezett kifejezést, hogy abból egy darab is elég a célok teljesítéséhez, lényegesen csökkentve ezzel a költségeket. Számos olyan single-term séma látott már napvilágot [Fer94] [EO95] [Fer95], amely mentes az előző pontban látott problémáktól.

Például a [Fer94] sémában az érmét három szám, $C = f_c(c)$, $A = f_a(a)$ és $B = f_b(b)$, és két tanúsítvány $(C^kA)^{1/v}$ és $(C^UB)^{1/v}$ reprezentálja, ahol a, b, c és k csak az ügyfél által ismert három véletlen szám, $1/v$ a bank titkos kulcsa, U a vásárló azonosítója (ID). A banknak alá kell írnia két tanúsítványt, miközben nem ismeri k-t, de meggyőződik arról, hogy U a felhasználó helyes identitása. A bank készíti el az érme alapját, de ezután a felhasználó bizonyos faktorokhoz véletlen kitevőket ad. Végül a felhasználó megkapja az elkölthető érméket, az ilyen pénzkivét protokollt közvetlen pénzkivétnek (direct withdrawal) is nevezik.

A fizetési fázisban a vásárló elküldi az a, b és c-t az üzletnek. Az üzlet visszaküld a vásárlónak egy véletlenül választott x kihívást (challenge). A vásárló ezután elküldi az $r = kx + U \ (mod\ v)$-t az üzletnek egy aláírással együtt: $(C^rA^xB)^{1/v} = \left((C^kA)^{1/v}\right)^x * \left((C^UB)^{1/v}\right)$. Az üzlet le tudja ellenőrizni, hogy mindezek az adatok egymással konzisztensek. Ha az érmét kétszer költik el, akkor két különböző x kihívást használnak a protokoll során. Így a banknak két pontja van az $X = Ux + k$ egyenesen (ami U-ra megoldható), hogy a felhasználó kiléte kiderülhessen. A korábban említett megoldások alkalmazhatók az ugyanolyan kihívású, ugyanazt a pénzt elköltő protokoll menetekben résztvevő felek ellen.

Ez a technika csak két szorzást és egy hatványozást igényel az *n* darab rejtjelezéssel szemben, az érmék tárolására is jóval kisebb hely elegendő. A gond csak az, hogy a pénzkivételi fázis bonyolult, ezért bonyolultabb matematikai bizonyítást igényel, hogy az ügyfél nem tud hamis *U* identitáshoz pénzt kivenni. A multiple-term séma jól ismert kriptográfiai protokollokat használ, amelyek már elég régen ismertek ahhoz, hogy biztonságukban megbízzunk. A teljes bizonyítás itt azonban még várat magára.

3.10. Hatékonysági problémák, költségek

Az off-line fizetőeszközök alkalmazásának már akkor is költségvonzata van, ha nem fordítanak gondot a privacy védelmére. A dupla költés érzékelése miatt a banknak minden érméhez el kell tárolnia a pénzkivételeknél és a pénzbeváltásoknál keletkező információkat egy adatbázisba. A rendszer természetéből fakadóan az összes számlatulajdonos fizetési története bitről-bitre le van tárolva. Ezek az adatok nagy szenzitivitású személyes adatok, amelyek óriási értékkel bírhatnak bizonyos érdekeltségek számára. Ha nem vetnek be kriptográfiai eszközöket a védelmükre (és itt az anonimitást értem az alapvető adatbiztonsági követelményeken túl), akkor nemcsak „nem privacy-védő” rendszernek, hanem egyenesen „privacy sértő” rendszernek bélyegezhetők.

Az adatbázis elég nagy terhelésnek van kitéve, hiszen minden digitális érme beváltásakor végig kell futtatni egy keresést rajta. Ha az alkalmazott digitális aláírás esetében feláldozzuk a biztonság matematikai bizonyíthatóságának egy részét, és Fiat-Shamir vagy Schnorr aláírást alkalmazunk, akkor az általános vélekedés szerint mind hatékonysági, mind biztonsági szempontból kielégítő rendszert kapunk.

Ha most az eddigiekbe még anonimitást és követhetetlenséget (untraceability) is bevezetünk, akkor annak szintén költségvonzatai vannak. Az első típusú esetben one-show vak aláírást alkalmaznak általában. A realizálás nem egyszerű, ugyanis a bank számára nem látható módon kell beágyazni egy érmébe a tulajdonos kilétét, úgy, hogy a bank ellenőrizni tudja a beágyazott információk és az érme formátumát és helyességét. A cut-and-choose protokollnak (3.6. fejezet) igen jelentős a kommunikációs és a számítási igénye. A korlátozott vak aláírás (3.13.1. fejezet) az első olyan megoldás, amelynél a bank számítási igénye a Schnorr aláírás számítással összevethető, és a bank által nyilvántartandó adatbázis nagyjából akkora, mint a privacy-sértő megoldásoknál. Sajnos a [Bra93] anonimitásának és biztonságának bizonyítása nem teljes, vannak csak részben bizonyított feltételezések. A [Bra93]-el egy időben megjelenő Ferguson séma [Fer94] sem igényel cut-and-choose technikát, azonban ennek a bizonyítottsága még gyengébb, még jobban megkérdőjelezhető.

3.11. Tökéletes bűntény

A 90-es évek elején még javában folytak a tökéletes anonimitású rendszerekkel kapcsolatos kutatások, de már ekkor megjelentek az akkori rendszerekkel szembeni bizonyos ellenérvek. Egyrészt látszott, hogy az aláíráson alapuló sémáknál rendkívül nehezen lehet kiküszöbölni a bankrablásos támadásokat (4.1.8. fejezet) [JY96].

Másrészt a legerősebb aggodalom a tökéletes anonimitás miatt fogalmazódott meg. Solms és Naccache [SN92] publikációjukban felidéztek egy megtörtént esetet. Az 1970-es évek elején Japánban egy „Kobayashi" néven elhíresült bűnöző számlát nyitott egy bankban. Ezután elrabolta egy híres japán tévésztár csemetéjét, és azzal fenyegetőzött, hogy megöli a gyermeket, ha nem utalnak 5 millió jent a megadott számú bankszámlára. Persze a „Kobayashi" név egy hamis személyiségnek bizonyult. Végül a rendőrségnek sikerült elfogni a zsarolót, azonban ehhez óriási erőfeszítésre volt szükség. Minden tokiói ATM automata közelébe rendőröket vezényeltek. A bank központi számítógépén beavatkoztak a számítógépes vezérlő programba, hogy valós időben figyelhessék, melyik ATM-nél vesznek ki pénzt a szóban forgó bankszámláról.

Solms és Naccache bemutatják, hogy mi történhetett volna tökéletesen anonim pénzrendszer esetén. A feltételezett bűnöző, ha elég intelligens, és érti a digitális pénz protokollját, akkor a bankot arra kényszeríthette volna, hogy mondjuk egy napilapban, nyilvános módon tegye közzé az általa kívánt kriptográfiai paramétereknek és kulcsoknak megfelelő kriptográfiai értékeket. Ezek segítségével érvényes érméket tudott volna saját maga számára előállítani.

A megtörtént tokiói esetben az tette lehetővé a bűnöző kézre kerítését, hogy az általa használt kreditkártya egyedileg azonosítható volt, amely egyértelműen hozzákapcsolta őt ahhoz a bankszámlához, ahova a pénzt el kellett helyezni számára. Sajnos tökéletes anonim rendszer esetén a vak aláírás protokoll miatt egyik elköltött érmét sem lehet kapcsolatba hozni a bűnözővel. A fiktív támadást emiatt „tökéletes bűntény" (perfect crime) névvel is illetik.

Ez a példa nagy erkölcsi nyomás alá helyezte a kutatókat. Technikailag megoldhatóvá kellett tenni, hogy kivételes esetekben az anonimitást vissza lehessen vonni. Hogy fogyasztóvédelmi oldalról ne adódjon ok aggodalomra, természetesen csak úgy lehet lebonyolítani a nyomkövetési eljárásokat, hogy azokat a bank ne végezhesse el önállóan, kizárólag megbízott harmadik felek segítségével legyen az megvalósítható. Így a bank nem élhet vissza a birtokában lévő információkkal, nem végezhet önkényesen megfigyeléseket.

Annál jobb, minél több fél szükséges a követések elvégzéséhez, mert így annál több egymástól független szervezet vesz részt ebben, így kisebb a kompromittálás kockázata.

3.12. Fair anonim rendszerek

Megszülettek az ún. fair anonimitású rendszerek, melyek válaszlépésnek tekinthetők a [SN92] által felvetett problémákra. Más terminológiával ezeket irányítható anonimitásúaknak (controllable anonymity) is nevezik. Az anonimitás visszavonásához valamilyen TTP-t (trustee, ombudsman nevekkel is illetik) vonnak be a folyamatba, amely a bank rendelkezésére bocsátja a követéshez szükséges adatokat. A visszavonható anonimitású rendszerekre a következő megállapításoknak igaznak kell lennie [CPV99]:

1. Az anonimitásnak visszavonhatónak kell lennie, de csak a trustee által, és csak az igényelt esetekben.
2. A trustee a követésen kívül nem képes másra a rendszerben.
3. Az anonimitás csak és kizárólag arra a tranzakcióra vonható vissza, amelyre a trustee utasítást kap (a törvényes szervektől).
4. A trustee-nak lehetőség szerint csak a visszavonás esetén kell közreműködnie, más esetekben off-line marad.
5. Az anonimitás-visszavonásnak lehetőség szerint nem szabad súlyosabb bűncselekményekre motiválnia annál, mint amilyenek ellen véd.

[BGK95] mutatta be az első trustee alapú nyomkövetést. A publikációban két bizonyíthatóan biztonságos, off-line rendszert ([Bra93] és [FY92]) terjesztettek ki fair anonim off-line fizetési rendszerré. Az eredeti rendszer felhasználói anonimitásának bizonyíthatósága megőrződött kivéve, amikor egy nyilvánosan kijelölt trustee segítségével a hatóságok nyomkövetést végeztek. A [BGK95]-ben bemutatott nyomkövetés csak a szükséges információkat hozza napvilágra, oda- és visszakövetés is lehetséges. A megoldás on-line vagy off-line rendszerben is implementálható.

A [BGK95] nyomkövetési mechanizmus hatékony, tulajdonképpen letétbehelyezés típusú megoldás. Mindkét típusú kiterjesztés azon alapul, hogy a felhasználó periodikusan rejtjelezett formában elküldi a tranzakciós adatait egy ún. ARDM (Automatic Records Deposit Machine) számára. Az adatok rejtjelezett formában tárolódnak, olyan módon, hogy csak két trustee együttes jelenlétével legyenek felfedhetők.

A „fair anonim” fizetési rendszer kifejezést először [CPS96] vezette be, ami valójában a [BKG95] trustee alapú nyomkövetéses rendszerének felel meg.

3.12.1. Anonimitás-visszavonási algoritmusok

Kezdetben kétféle anonimitás-visszavonás állt rendelkezésre, attól függően, hogy milyen bemeneti információt kap a művelethez a trustee.

1. Pénzkivét alapú anonimitás-visszavonás: a bank által a pénzkivét tranzakció során látott nézeten (view) alapul. A trustee egy olyan információdarabot számol ki, melynek segítségével a bank felismerheti a későbbi elköltéskor a szóban forgó kivett pénzt. Más terminológiában ez az érme-nyomkövetésnek (coin tracing) felel meg. Ha egy felhasználót zsarolnak, akkor az titokban szólhat a banknak, és így az érme-nyomkövetéssel felismerhetik elköltéskor a támadót. Ez hasonló ahhoz, mint amikor hagyományos pénznél az egyes bankjegyek sorozatszámait feketelistára helyezik.
2. Fizetés alapú anonimitás-visszavonás: a bank által a pénzbeváltás tranzakció során látott nézeten (view) alapul. A trustee egy olyan paramétert számol ki, ami egy adott pénzkivéthez kapcsolható. Erre esetleg pénzmosás gyanújának felmerülésekor lehet szükség. Más terminológiában ezt pénzkivétel-nyomkövetésnek (withdrawal tracing) vagy tulajdonos-nyomkövetésnek (owner tracing) is nevezik.
3. Később kialakult egy harmadik mechanizmus is, ami megmondja egy adott pénzkivétel és fizetési nézethez, hogy azok összetartoznak-e, tehát egy eldöntendő kérdésre ad egy igen/nem választ. Ez a fajta funkció jól jöhet bizonyos esetek felderítésénél.

Fontos az a követelmény, hogy a trustee ne játszhassa el senki más szerepét a rendszerben. Így ha a trustee kulcsa kompromittálódik, akkor a rendszerben a vásárlók anonimitása megszűnik, de a bank szempontjából a rendszer biztonságos marad, a trustee nem tud pénzt hamisítani.

A [CMS96] előtti fair anonim digitális pénzrendszerek nem voltak hatékonyak vagy a cut-and-choose paradigma alkalmazása miatt [BGK95, SPC95] vagy azért, mert megkövetelték a trustee részvételét a számla nyitásakor, vagy esetleg minden pénzkivét protokoll során [SPC95, CPS96, JY96].

Működési szempontból fontos elvárás, hogy a trustee passzív lehessen, azaz ne legyen szükséges a részvétele a mindennapi tranzakciókban. Akár az is lehetséges, hogy még a számlanyitáskor se legyen jelen, hanem csak a rendszer inicializálásakor, és gyanús esetek felmerülésénél a nyomkövetésben működjön közre.

Hatékonysági szempontból fontos, hogy a TTP a fizetési protokoll mely fázisaiban és milyen módon vesz részt. Három fő típust lehet elkülöníteni ennek alapján.

1. A trustee minden pénzkivét során jelen van, tulajdonképpen a felhasználó nevében viszi véghez a „vakolási" fázist [JY96], [SPC95]. A trustee triviálisan vonhatja vissza az anonimitást szükség esetén.
2. A trustee a bankszámlák nyitásánál van csak jelen. Az ilyen rendszerek hatékonyabbak, mivel egy bankszámlát általában több tranzakcióhoz is használnak [CPS96].
3. A trustee nem vesz részt a protokollokban, csak az anonimitás-visszavonásnál jelenik meg. A vásárló valamilyen zero-knowledge paradigma segítségével bizonyítja a banknak, hogy az érme olyan információkat tartalmaz a trustee nyilvános kulcsával kódolva, amelyek segítségével az anonimitás visszavonható.

A harmadik kategóriába eső rendszerek [SPC95] nem voltak hatékonyak. A [CMS96] nem igényli a trustee-tól egyik tranzakcióban való részvételt sem, és egyéb számításokban is hatékony. Ezzel párhuzamosan készült egy ugyanilyen követelményeket teljesítő hasonló rendszer, a [FTY96].

Az anonimitás-visszavonás csökkentheti a csalások számát, de olyan lehetőségeket is teremthet, ahol a bűncselekmény súlyossága nő (3.16. fejezet). Ennek megakadályozására [DFTY97] a vészjelzéses pénzt javasolja, egy támadó által észrevehetetlen módját a törvényhozás által elrendelt nyomkövetés aktiválásának.

3.13. Fair-séget biztosító aláírás sémák

Mivel a klasszikus vak-aláírás sémák tökéletes összeköthetetlenséget biztosítanak, ezért ezeket bűnözők rossz célokra használhatják (tökéletes váltságdíj-követelés, pénzhamisítás [SN92]). Bár a tökéletes anonimitás az egyén privacy-jének védelmében elvben kívánatos lenne, de be kell látni, hogy a zsarolásos tökéletes bűntény véghezvihető, ezért mindenképpen valamilyen megoldást kell találni erre a problémára. Megoldás lehet egy olyan módszer, ami kriptográfiai eszközökkel eléri, hogy a becsületes felhasználók anonimitása ne sérüljön, bűntény esetén azonban a gyanúsított identitása kideríthető legyen. A tökéletes anonimitás szemszögéből nézve ez egy kompromisszumos megoldás, amit a lehető legmegnyugtatóbb módon kell rendezni. Ennek a megoldására kísérletezték ki a kutatók a különféle fair anonimitást biztosító eszközöket. A fair anonimitás eszközök többféle nyomkövetési algoritmus segítségével (érme- és tulajdonos-nyomkövetés) támogatják a bűncselekményeket felderítését.

3.13.1. Korlátozott vak aláírás (restrictive blind signature)

Szemléletesen ezt olyan protokollnak képzelhetjük el, ahol a fogadó az *m* üzenet „külsejét” (és az aláírást) „vakolni” tudja, de az *m* belső szerkezetét nem. Ebből fakad az elnevezés is.

Világos, hogyha egy számlatulajdonos az *m* üzenet belső struktúráját is képes „vakolni”, akkor nem lesz felderíthető a kiléte egy esetleges csalás után. Ezért feltétlenül szükséges, hogy a fogadó a „vakolási” módosítást csak korlátozottan tudja megtenni, ami a korlátozott vak aláírás terminológiának a magyarázata.

Sajnos ez a rendszer csak részben bizonyított feltételezéseken alapul: az, hogy a vásárló az érmébe megfelelően belekódolja az identitását, nem bizonyítható teljesen. Az aláírás hamisíthatatlanságát Pointcheval és Stern 1996-ban bizonyította.

3.13.2. Reprezentációs problémán alapuló korlátozott vak aláírás

Brands a [Bra93]-ban mutatott be először ilyen építőelemet. Matematikailag egy saját problémán, a prím rendű csoportok feletti reprezentációs problémán alapul (representation problem of groups in prime order) a biztonsága. Mindezt egy megfigyelővel ellátott smart card-os rendszerben képzelték el (wallets-with-observer), a rendszer off-line fizetéseket is lehetővé tesz.

A [Bra93]-ban olyan rendszert mutatnak, ahol fizetési protokoll során a számlatulajdonosnak nemcsak az *A*-t és az aláírást kell felmutatnia, hanem bizonyos részinformációkat az A reprezentációjáról is. Ez a részinformáció nem fed fel shannoni értelemben semmi információt az u_1-ről (belső szerkezetéről), de két ilyen részinformáció ismerete lehetővé teszi a bank számára, hogy u_1-et polinom idejű algoritmussal kiszámítsa. Így ezzel a módszerrel a dupla költés nyomkövethető.

A [Bra93] konkrét korlátozott vak aláírás sémája eredetileg a Chaum-Pedersen [CP92] vak aláírás kiadási protokollból származtatható. Egy nyilvános-kulcs tanúsítvány séma, azonban annak speciális változata. Brands és mások azon törekvése, hogy egy ilyen típusú másik konkrét sémát találjanak, meghiúsult. A nehézség a tervezésnél ott adódik, hogy ezekben a rendszerekben a nyilvános kulcs és az ahhoz tartozó tanúsítvány között egy speciális, nagyon szoros kapcsolatnak kell fennállnia.

A biztonság csak részben bizonyítottan vezethető vissza a Schnorr aláírásra, illetve a Diffie-Hellman feltételezésre. Wallets-with-observers paradigma realizálásánál a pénzkivétnél és

pénzbetétnél is tulajdonképpen a Schnorr azonosítási protokoll játszódik le. A csalások elleni védelem a DLA-n alapul. Ez erősebb, mint az ugyanilyen felépítésű Okamoto séma Schnorr aláíráson alapuló biztonsága. A Brands-féle off-line sémát [Bra94] szintén részletesen mutatja be.

3.13.3. Titkos-kulcs tanúsítványon alapuló korlátozott vak aláírás

Később Brands bemutatott egy titkos-kulcs tanúsítvány (secret key certificate) elnevezésű technikát [Bra95b]. A titkos-kulcs tanúsítvány alkalmazásánál az aláíró látja az összes attribútumot, de a tanúsítványhoz tartozó aláírandó kulcsot nem. A tanúsítvány tulajdonosa számára lehetővé válik annak megválasztása, hogy a tanúsítvány-ellenőrző félnek mely attribútumokat mutassa meg. Vagyis a felhasználó eldöntheti, hogy az ellenőrzőnek mennyi és milyen információt szolgáltat ki. Ráadásul az aláíró nem látta az aláírt nyilvános kulcsot. Ez megakadályozza, hogy a tanúsítvány kiadója össze tudja kapcsolni a nyilvános kulcsot a tanúsítvány tulajdonosával. A tanúsítvány-ellenőrzők pedig nem tudják összekapcsolni ugyanazon tanúsítvány különböző felhasználásait, és nem tudnak felhasználói profilokat készíteni.

A [Bra95b] titkos kulcs tanúsítvány technika már sokkal alkalmasabb korlátozott vak aláírás sémák tervezésére, mint a nyilvános-kulcs tanúsítványokon alapuló módszerek. Nevezetesen, ez alkalmas bármely olyan Chaum-Fiat-Naor típusú aláírás séma korlátozott vak-aláírás sémává alakítására, amely az Okamoto-Ohta technika [OO92] alkalmazásával vak-aláírás sémává tehető. Az eredményül kapott sémáról kizárólag standard feltételezéseken alapulva, matematikailag bebizonyítható, hogy „korlátozottan vak”. Ezek az új sémák mind on-line, mind off-line alkalmazásokban hatékonyabbak, mint az előző.

Kissé meglepő módon, ezek az új aláírás sémák nem hagyományos értelemben vett vak-aláírás sémák. Tekintsük a következő hármast: titkos kulcs, a hozzá tartozó publikus kulcs, tanúsítvány a publikus kulcshoz. A pénzkivét protokoll során a felhasználó képes „vakolni” a publikus kulcsot és a publikus kulcshoz való tanúsítványt teljes egészében, azonban a privát kulcsnak csak egy részét képes „vakolni”. Ha a tanúsítvány egy hagyományos publikus kulcs tanúsítvány lenne (mint ahogyan az összes korábbi rendszer esetében van), akkor az egész séma valóban a „sima” „vakolt” aláírás sémák egy változata lenne (amelyben az üzenetet és üzenet aláírását „vakolni” lehet, lásd Chaum); a nyilvános kulcs az üzenet, a tanúsítvány pedig az üzenet aláírása.

Mindazonáltal, mivel a rendszerben bemutatott tanúsítvány egy titkos-kulcs tanúsítvány, definíció szerint ez nem egy aláírás egy publikus kulcson. Ebben az új közelítésben a titkos kulcs az üzenet, a tanúsítvány pedig egy aláírás az üzeneten. De az üzenet nem „vakolt”,

sőt, „vakolhatatlan”. A rendszer a titkos-kulcs tanúsítványok használatával cáfolja, hogy hatékony privacy-védő off-line pénz séma csak nyilvános-kulcs tanúsítványokon alapulhat, és hogy a pénzkivét protokoll csak a hagyományos vak-aláírás sémákat használhatja.

3.13.4. Gyenge vak aláírás (blind weak signature)

Az [FY94a] [FY94b] megoldása a fair pénzrendszer követelményekre egy olyan séma alternatíva, ahol a rendszer nem tartalmaz hagyományos digitális aláírás számítást. Ez egy on-line rendszer, ahol a pénzkivét fázisban a bank egy trustee-val közreműködve egy ún. gyenge (weak) aláírást készít, illetve a pénzbetét fázisban a trustee (TTP) segítségével ugyanezt ellenőrzi. A módszer matematikája véges elemű algebrán alapul. A trustee-nak on-line-nak kell lennie a pénzkivétnél és a pénzbetétnél is. Az érmekövetési algoritmus egyszerű.

A technika alapját képező gyenge aláírásokat Rabin és Ben-Or publikálta válaszul egy több-résztvevős biztonságos kommunikációs problémára, amelyhez olyan megoldást adtak, ahol trustee részvételével történhet a hitelesítés. Rabin megmutatta, hogy a check vector technikával egyszerűen implementálható is az algoritmus. [FY94] pedig megmutatta, hogy a gyenge aláírások könnyen „vakolhatóak”, és az így keletkezett séma on-line fizetési rendszerekben alkalmazható. A módszer biztonsága csak a vektorok linearitására épül, és érdekes módon nincs szükség kriptográfiai feltételezésekre, mint a legtöbb sémában.

Ezzel a check vektor módszerrel egyébként a cut-and-choose algoritmusokhoz hasonlóan egy támadó véges valószínűséggel végrehajthat sikeres csalást. Jelen esetben 1/(p–1), ahol p egy nagy szám, tehát az esély kicsi, de nem zérus. Az üzenetküldő tárolási költség nem függ p-től, de lineárisan függ egy k biztonsági paramétertől. Ezenkívül a rendszer hátránya a kizárólagos on-line működési képesség is.

3.13.5. Fair vak aláírás (fair blind signature)

A fair vak aláírás séma [SPC95] a vak aláírások új típusa: egy olyan plusz tulajdonsággal rendelkezik, hogy egy megbízott harmadik fél segítségével össze lehet kapcsolni az üzenet-aláírás párt és az aláíró által látottakat, és ezáltal fel lehet fedni az eltakart információkat egy adott aláírás esetén. Az egész sémában van egy új résztvevő, az ún. megbízott harmadik fél (TTP, trustee), aki birtokába jut olyan információknak, melyek segítségével az anonimitás-visszavonás megtehető.

A fair vak aláírás séma modellje számos küldőből (sender), egy aláíróból (signer), egy megbízott félből (TTP, például bíró), és két protokollból áll:

- aláírási protokoll a küldő és az aláíró között: a küldő érvényes aláírást szerez egy általa választott üzenetre, úgy, hogy az aláíró az általa látottakat nem tudja összefüggésbe hozni az üzenet-aláírás párral;
- kapcsolatfelfedő (link recovery) protokoll az aláíró és a TTP közreműködésével: az aláíró információt kap a TTP-tól, ami lehetővé teszi számára, hogy felismerje a protokoll futamhoz tartozó aláírás-üzenet párt.

Több kapcsolatfelfedő protokollt különböztetünk meg attól függően, hogy a bíró milyen információt kap az aláírótól a protokoll során.

- Type I: Adott egy aláíró egy menet során látott információja. A TTP ehhez egy olyan információt szolgáltat, ami lehetővé teszi az aláíró (vagy bárki) számára, hogy hatékonyan felismerje a látott információhoz tartozó üzenet-aláírás párt. Ez tulajdonképpen az érmekövetési eljárást biztosítja.
- Type II: Adott egy üzenet-aláírás pár. A TTP olyan információt szolgáltat, ami az aláírónak lehetővé teszi, hogy hatékonyan azonosítsa az üzenethez tartozó küldőt, vagy megtalálja az ehhez a protokollhoz tartozó nézetét (view). Ez tulajdonképpen a tulajdonos-nyomkövetési eljárást jelenti.

Elméletileg egy Type I fair vak aláírás séma Type II módon is működhet, ha a kapcsolat-felfedő protokollt az összes nézetre (view) mint inputra végrehajtjuk, de ez nagyon költséges, és az anonimitást is megsérti. Hasonló állítás igaz a Type II sémákra is. Ezért a fair működés érdekében a sémának mindkét nyomkövetéshez külön cél-algoritmussal kell rendelkeznie.

A Type II sémán alapuló fizetési rendszerek esetén a hatóságok meg tudják állapítani egy gyanús pénz eredetét, míg Type I séma alapú rendszereknél megvizsgálhatják a gyanús pénzkivét protokollok célját. A Solms-Naccache-féle tökéletes bűntény esetén is alkalmazható: ha egy vásárlót azzal zsarolnak, hogy anonim módon váltson ki pénzt, ezáltal közvetítőként viselkedik a bank és a zsaroló között. Ha a rendszer Type I típusú, akkor a TTP a bank protokoll nézetének ismeretében vissza tudja követni a pénz útját. Sajnos nem minden fair vak aláírás megvalósítás küszöböli ki a „tökéletes bűntényt": egy csaló küldő arra kényszerítheti az aláírót, hogy az eredeti helyett egy nem szabványos, ténylegesen anonim vak aláíró algoritmussal vegyen részt a protokollban. Ennek a problémának a megoldása nehéznek tűnik.

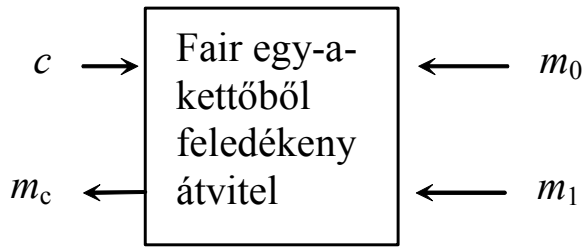
Az [SPC95]-ben háromféle fair aláírás sémát mutatnak be. Az első típus cut-and-choose alapú, ugyanis ilyen módszerrel győződik meg az érmék megfelelő formátumáról.

A hagyományos cut-and-choose annyival van kiegészítve, hogy a protokoll lépések közben a küldő a TTP publikus kriptográfiai rendszerével is rejtjelez egyes elemeket. A TTP így tud később a követésekben segíteni. A séma mind Type I, mind Type II típusú. A következő séma a Fiat-Shamir aláíráson és a fair feledékeny átvitelen alapszik.

Az [SCP95] nem ad megnyugtató megoldást a zsarolásos támadások kivédésére, illetve a bemutatott példák nem hatékonyak.

3.13.6. Fair egy-a-kettőből feledékeny átvitel (fair one-out-of-two oblivious transfer)

Az egy-a-kettőből feledékeny átvitel Even, Goldreich és Lempel-től származik. Olyan kriptográfiai protokoll egy küldő és fogadó fél között, ami lehetővé teszi a vevő számára, hogy válasszon egy üzenetet a küldött kettő közül, úgy, hogy egyrészt csak a kiválasztott álljon rendelkezésére, másrészt a küldő ne tudja meg, hogy melyiket választotta (4. ábra). Az ábrán a feledékeny átvitel látható, m_0 és m_1 a két küldött üzenet, c a választó bit, m_c pedig a választott üzenet.



4. ábra: Feledékeny átvitel

A fair feledékeny átvitel ennek a protokollnak egy olyan módosított változata, melyben egy TTP külső fél mondhatja meg, hogy a vevő melyik üzenetet kapja [SPC95]. A QRA feltételezés (kvadratikus maradék) értelmében a küldő nem képes megállapítani a vevő által választott üzenetet, ellenben a TTP ezt megteheti. A vevő a Diffie-Hellman feltételezés (DHA) értelmében nem képes meghatározni a másik üzenetet sem.

A fair feledékeny átvitel segítségével a Fiat-Shamir típusú aláírások Type I típusú fair aláírássá alakíthatók. Az aláírás séma vak és fair típusú is [SCP95].

[SPC95] harmadik példája egy olyan rendszert vázol fel, ahol a felhasználók különböző pszeudonímekkel regisztrálnak a TTP-hez. Ez a séma tulajdonképpen egy Chaum-Pedersen

[CP92] vak-aláírás séma módosításának tekinthető. Ennélfogva a biztonsága és a vak tulajdonsága erős összefüggésben van annak a tulajdonságával. Megjegyzendő azonban, hogy a [CP92] rendszere manipulálás-védett eszközt és beágyazott megfigyelőt is tartalmaz, és az anonimitási tulajdonságai nem kiforrottak, ezt a rendszert [CP93b] (Cramer-Pedersen) továbbfejleszti.

3.13.7. Indirekt diskurzus bizonyítékok (indirect discourse proofs)

Az ún. indirekt diskurzus bizonyíték egy [FTY96] által elnevezett és kitalált technika FOLC implementálására. [FTY96] olyan sémát mutat be, ahol a trustee-nak nem szükséges a pénzkivét protokollban részt vennie. A [CPS96] ezzel egy időben készült, ugyanazokat a tulajdonságokat teljesíti, azonban mintegy kétszer hatékonyabb kommunikációs és számítási teljesítményben is. Fontos különbség azonban, hogy a nyomkövetéshez a [CPS96]-ban a pénzkivét adatbázisban, míg [FTY96]-ban csak a jóval kisebb bankszámla adatbázisban kell keresést végrehajtani. A pénzt kivevő felhasználó az indirekt diskurzus bizonyíték segítségével bizonyítja a fizetés során, hogy igény esetén a személy nyomkövethető.

A trustee aktív részvételét úgy küszöbölik ki, hogy a protokoll lefutása során bizonyítást nyer, hogy lehetséges aggályok, támadások vagy viták esetén a trustee képes megtenni a szükséges lépéseket. A bizonyítás során használt bizonyítékok az indirekt diskurzus bizonyítékok. A bizonyítékban a bizonyító fél a TTP egy kriptográfiai képességére hivatkozik anélkül, hogy a TTP-t segítségül kellene hívni ehhez a bizonyítási eljárás alatt.

A [FTY96]-ben a [Bra93] rendszert módosítják, s így jutnak el egy FOLC sémáig. A séma új tulajdonsága a trustee-k passzív részvétele. A bizonyíték lehet másoknak nem átadható, illetve átadható. Az első példák nem átadhatóak, mint ahogyan a [DFTY97]-ben szereplő sem, azonban ott a módszer hatékonyságát növelik, költségét csökkentik.

A [FTY98] publikációban a technika biztonságát erősebb feltételezésekre építik, elfogadhatóbban bizonyítják. Másik fejlesztés, hogy itt a fizetési protokoll, melynek során a bizonyítékot is át kell adni, már non-interaktív lehet.

Ebben a konkrét sémában a bizonyíték logaritmusok egyenlőségének bizonyításaival (proof of equality of logarithms) valósul meg. Maga a logaritmusok egyenlőségének bizonyítása párhuzamos Schnorr knowledge proof-ok halmaza, és akár egyszerre több logaritmus egyenlőségének bizonyítására is használható. Mint ahogy a Schnorr aláírás esetében is (3.2.2. fejezet), ez is non-interaktívvá tehető.

3.13.8. Mágikus tintás aláírás (magic ink signature)

Tekintsük a hagyományos vak aláírást: az aláírás „kivakolására” itt csak az aláírás-fogadó képes. Előfordulhat a digitális pénzrendszerben, hogy szükségessé válik az aláírás „kivakolása”. Ha ezt maga az aláíró is meg tudja tenni, akkor ez egy anonimitás-visszavonási műveletnek tekinthető.

Jakobsson mágikus tintás aláírás sémájára a következő fizikai analógia képzelhető el. Az aláíró elhelyez egy papírlapot rajta egy indigópapírral egy borítékba. Ezek után az aláírás fogadó ráírja a dokumentumot a borítékra egy olyan mágikus tintával, amely láthatatlan. Az indigó miatt a borítékban lévő papírra a dokumentum látható módon kerül rá. Ezek után az aláíró aláírja a borítékot. A fogadó megszerzi a belső papírlapot, az aláíró viszont megőrzi a borítékot, rajta a mágikus tintás másolattal. Ha az aláírónak szüksége lenne az aláírt dokumentumra, akkor speciális feltételek mellett láthatóvá tudja tenni a mágikus tintát. Az aláírás tehát nem örökre „vakolt” az aláíró előtt. Ezt a fajta aláírást nevezzük mágikus tintás aláírásnak.

A mágikus tintás aláírásra Jakobsson és társai a szabványosított DSA (Digital Signature Algorythm) [FP186] aláírásra alapozva adnak elvi implementációt. Habár a [Jak97] egy szerveres megoldást mutat, de a kifejezetten csak a mágikus tintás aláírással foglalkozó [JY97] bemutatja, hogy hogyan lehet elosztott algoritmus segítségével MI-DSS-t generálni, úgy hogy a szerverek bizonyos csoportja vesz részt az aláírásban, míg egy másik csoport lehet képes az aláírás „kivakolására”. A séma robosztus, a műveletek akkor is garantáltak, ha a csoportokból egy adott határértéket meg nem haladó számú résztvevő visszautasítja az együttműködést, vagy csalással próbálkozik.

Mint általában a többi fair aláírás sémával, az MI sémával is mindkét típusú nyomkövetés lehetséges (egy adott aláírás session-ből vagy identitásból eljut a kért aláírásokig, illetve egy adott aláírásból eljut az aláíró session-ig vagy az identitásig). Itt lehetőség van a harmadik típusú nyomkövetésre is: meghatározhatjuk, hogy egy konkrét aláírás az adott session-nél lett-e kiadva vagy sem. Ez megkönnyít bizonyos követéseket anélkül, hogy a kérdéses válasznál több információt megtudnánk.

A [JM99]-ban több ponton is továbbfejlesztik a sémát. Az első és a harmadik követésnek a költsége nem függ a kiadott aláírások számától. A korábbi változatban a második megoldás költsége lineáris volt. Az új változatban ezt a költséget általános esetben logaritmikusra redukálják, csak nagyon valószínűtlen helyzetben válik lineárissá az algoritmus.

[JM99] a második fejlesztésével növeli a támadások elleni védelmet. A MI aláírások egyik fő előnye a többi fair sémával szemben, hogy lehetővé teszi az aláíró (bank) számára, hogy megkülönböztesse az érvényes aláírások közül azokat, amelyeket a bank adott ki, azoktól, amelyeket egy olyan másik fél készített, aki birtokolja az aláíró kulcsokat. Ez nagyon fontos szerepet kap egy esetleges „bankrablás" típusú támadásnál. Egy fejlesztés segítségével az ilyen eseteket még nagyon korai fázisban érzékelni lehet. Mindeközben a felhasználók anonimitása nem sérül.

A fejlesztések jó része egy ún. tipp értékek (hint value) technikán alapul. A tipp érték az aláírás fogadó által kapott aláírás rejtjelezéseként fogható fel. Számításelméletileg nem lehetséges egy támadó számára hatékonyan kiszámolni egy tipp értéket anélkül, hogy adott számú szervert ne korrumpálna, ugyanakkor adott számú szerver hatékonyan képes kiszámítani az értéket. Az aláírási eljárás során a felhasználó megkapja az aláírást, kiszámítja a tipp értéket és önként elküldi az aláíró feleknek. A felek eltárolják ezt a felhasználó identitása és más, a követéshez szükséges értékek mellett. A nyomkövetésnél (második típusú) a nyomkövető szerverek csoportja együttesen képes kiszámítani a tipp értéket, és megpróbálja megkeresni az adatbázisban az ezt tartalmazó rekordot. Ha nem találják meg, akkor a felhasználó által korábban adott tipp nem volt helyes, a nyomkövetést a korábbi lineáris algoritmus segítségével el lehet végezni.

Azért tipp ezeknek az értékeknek a jelzője, mert nagyon hatékony nyomkövetést tesznek lehetővé, másrészt hatékonysági okokból nem ellenőrzi a rendszer a helyességüket, így lehet, hogy nem „jönnek be". A felhasználó számára nincs jelentősége annak, hogy rossz értéket küldjön, és noha a pénzkivét folyamat során nem derül ki a tipp helytelensége, de a tiltott aláírásokat is érzékelő mechanizmus detektálja, s ekkor a felhasználó nyomkövethető és megbüntethető.

Általánosságban egy adott formátumú szám (mint a tipp érték) kiszámításának és ellenőrzésének tradicionális módja magában foglalja egy titkos érték megosztását. De ez drasztikusan megnövelné a részleges helyességre vonatkozó bizonyítások költségét, így egy merőben más utat választ Jakobsson és Yung. A titokmegosztás magas költségét és a robosztus számításokat kiküszöbölik azzal, hogy nyílt üzenet helyett a rejtjelezett adaton hajtanak végre manipulációkat. A keletkező aláírást ez nem befolyásolja, továbbra is DSS szerinti lesz. Ez egy olyan általános ötlet, ami könnyen lehet, hogy más kriptográfiai területeken is jól hasznosítható.

A felsorolt fejlesztések egyetlen hátránya az érintett felek kommunikációs és számítási költségeinek minimális növekedése, illetve az adatbázis méretének nem jelentős növekedése.

3.14. Csoport-aláírások, Fair csoport-aláírások

A csoport-aláírások elképzelését először Chaum és van Heijst publikálta 1991-ben. Tulajdonképpen tagság-hitelesítési sémák általánosításaként foghatók fel, ahol egy személy bizonyítja, hogy egy adott csoporthoz tartozik. A csoport-aláírás sémák lehetővé teszik a csoport tagjai számára, hogy a csoport nevében írjanak alá dokumentumokat úgy, hogy közben nem derül ki a konkrét aláíró kiléte. Az sem állapítható meg, hogy két adott aláírást ugyanaz a csoporttag készített-e. Az aláírás érvényessége egy darab ún. csoport nyilvános kulcs segítségével ellenőrizhető. Vitás esetekben egy TTP vagy egy kitüntetett csoporttag képes megállapítani, hogy az aláíró a csoport melyik tagja.

[CH91]-ben az anonimitás számításelméletileg garantált. Később Chen és Pedersen továbbfejlesztett néhány sémát és feltétel nélküli anonimitást ért el. Kidolgozták a csoporttagok felvételének lehetőségét és protokollját. A sémák biztonsága a legtöbb esetben matematikailag a DLA, dupla DLA, gyök DLA feltételezéseken alapulnak.

[Cam97] általánosított csoport-aláírásokat mutat be, amelyben csoporttagok egy koalíciója is képes a csoport nevében aláírni. Camisch és Stadler [CS97] olyan sémát mutatnak be egy publikációjukban, amely hatékonyabb az előzőeknél, mivel a csoportaláírás mérete független a csoport méretétől, így nagy csoportokra is hatékonyan alkalmazható.

Az előző csoport-aláírás sémákat a vak-aláírás sémákkal kombinálva [LR98] megalkotta a vak csoport-aláírásokat. Minden művelet független a csoport méretétől. Az általuk közölt séma hátránya, hogy on-line. Az off-line működés egy pénzrendszerben való felhasználásakor csak a vevő anonimitásának bizonyos gyengítésével érhető csak el.

[Pet97] megmutatja, hogyan konvertálható bármely aláírás séma csoport-aláírás sémává. Mindezt ráadásul határérték kriptográfiával együtt teszi, egy művelet elvégzéséhez meghatározott számú résztvevő félből elegendő, ha csak egy határértéket meghaladó számú résztvevő működik együtt. Természetesen megszülettek a vak csoport-aláírásoknak a határértékes megfelelői is.

Egyébként számos más csoport-orientált aláírás séma koncepció létezik a csoport-aláírásokon kívül. A legfontosabbak a proxy aláírások és a multi-aláírások. A Mambo, Usuda és Okamoto által először bemutatott proxy aláírások olyan aláírás sémák, ahol az eredeti aláíró az ő aláírási képességével egy proxy aláírót bíz meg, így a nevében végez el aláírásokat. A proxy aláírásoknak számos altípusa van, és az irodalmuk is egyre bővül. Multi-aláírás minden olyan aláírás, ami egynél több személytől függ. A multi-aláírásokat

általánosított csoport-aláírásoknak tekinthetjük, ahol nem lehetséges az aláírások kinyitása (a konkrét aláíró kilétének meghatározása). Jelenleg aktív kutatómunka folyik ezen a területen, egyre tökéletesebb sémák megjelenése várható.

3.15. A protokollok határérték kriptográfiával (threshold cryptography) való kiterjesztése

Intenzív kutatómunka folyik továbbá az ún. threshold kriptográfiai területeken. Ezek olyan protokollokat és algoritmusokat jelentenek, ahol egy adott cél érdekében több résztvevő fél vesz részt egy számításban. A célt csak akkor érhetik el, ha a résztvevő felek száma meghalad egy bizonyos határértéket, illetve ha a résztvevők közül legalább egy bizonyos határértéket meghaladó számú résztvevő jóhiszeműen, szabályosan, csalás nélkül viselkedik.

Az ilyen protokollokat nagyon sok helyen fel lehet használni az elektronikus fizetési rendszerekben. Általában a fizetési protokollok döntő többsége csak egyetlen bank jelenlétét feltételezi. Egy megvalósítható rendszer megalkotásához mindenképpen olyan alapmodellt kell tekinteni, ahol sok bank van jelen. Véleményem szerint a felhasználói és a másik oldalról is ott van az anonimitás és a fair-ség közötti határvonal, ahol az egyes fázisokban e két felen kívül még más pártatlan felek (például ombudsman) is részt vesznek. Az anonimitás-visszavonásra ez mindenképpen igaz. Hogy a jelenlegi sémákat ilyen rendszerekké terjeszthessük ki, szintén threshold kriptográfiára van szükség.

3.16. Distress cash (vészjelzéses pénz)

A nyomkövethetőség bevezetése volt a válasz a tökéletes anonimitással rendelkező pénzrendszerekben elkövethető tökéletes bűntényekkel szemben. A törvényhozási, kormányzati és nagyvállalati érdekekkel szemben állva azonban egyes kriptográfus szakemberek arra figyelmeztetnek, hogy ha másik oldalról szemléljük a dolgot, akkor a nyomkövethetőség bevezetésével akár még súlyosabb bűncselekmények megjelenésére lehet számítani.

Megfigyelték, hogy az autólopást gátoló kormánybilincs lehet, hogy csökkentette az autólopások gyakoriságát, de növelte a sokkal veszélyesebb autó-elrablások (car-hijacking) számát. Ezeknél úgy tulajdonítják el az autót, hogy a tulajdonos jelen van, és súlyosan bántalmazzák, leütik, vagy megölik a céljuk érdekében. A probléma olyan méreteket öltött, hogy az USA törvényhozók szövetségi offenzívát indítottak az autó-elrablások ellen. Ennek analógiájára az érme-nyomkövethetőséggel rendelkező fizetőeszközök esetén a bűnözők lehet, hogy az áldozat elrablásához vagy esetleg a megöléséhez folyamodnak, mert minél nagyobb késleltetést szeretnének elérni a megszerzett pénz elköltése és a nyomkövetési

eljárás megkezdése között. Nyilvánvalóan, ha a bűnöző megöli a felhasználót, akkor kiterjesztheti azt az időtartamot, ami alatt a lopott digitális pénzt felhasználhatja.

A fenti problémára egy megoldást jelenthet egy védett jelzési csatorna alkalmazása a pénzkivét során [DFTY97]. A csatorna potenciálisan be van ágyazva a protokollba, így a felhasználó mindig jelezhet a banknak, ha szükséges. Ennek realizálásának egyik egyszerű lehetséges megoldása, ha felhasználó-azonosítási protokoll egy smart card-ba van beágyazva, úgy, hogy a felhasználónak két PIN-je (Personal Identification Number) van. Az egyik PIN a normál használatra szolgál, a másik PIN-el pedig az előző funkcionalitás mellett észrevétlenül vészjelet küldhet a banknak egy leplezett titkos csatornán keresztül.

A jelzésre egy fejlett megoldás képzelhető el Simmons fegyenc-dilemma protokolljára alapozva (prisoners' dilemma). Az eredeti dilemmában két fegyenc úgy egyeztet alibit egymással, hogy az üzenetekre alkalmazott aláírás sémákba rejtett csatornát létesítenek. A fegyőr sejti a dolgot, de nem tudja felfedni a csatornát. Jelen esetben a bank és a felhasználó a fegyencek, és a bűnöző a fegyőr. A felhasználó a hitelesítési csatornáján keresztül e protokoll segítségével jelet küldhet, mely a bűnöző számára rejtett marad. Ha a pénzkivét protokollban a felhasználó aláírása is megjelenik, akkor a rejtett csatorna beágyazható ebbe, hogy veszélyt jelezhessen, és megindulhasson a nyomkövetés.

3.17. Atomicitás

[Tyg96a] [Tyg96b] [ST96] Az elektronikus fizetési rendszerek területe rengeteg munkát inspirált, de sajnos a nagy részük nem alkalmazza a tranzakció-feldolgozás tudományának eredményeit. Ezek közül a legalapvetőbb az atomicitás.

Az atomicitás annyit jelent: több operáció logikailag egy egységgé kapcsolható össze, tehát vagy mindegyik végrehajtódik, vagy egyik sem. Mivel a tranzakciós rendszer elosztott környezetben fut, ezért bármilyen (például hálózati kommunikációs) hiba esetén a résztvevő felek vissza tudnak kerülni (roll-back) a félbemaradt vagy hibásan lezajlott művelet utáni inkonzisztens állapotból a tranzakciót megelőző konzisztens állapotba.

Az atomikus tranzakciók a modern tranzakció-feldolgozási tudomány egyik sarokkövét jelentik, óriási mennyiségű kutatómunka kapcsolódik hozzájuk. Az „A” az „ACID tranzakció” kifejezésben az atomicitást jelenti. Nem atomikus elosztott tranzakciós rendszert az adatfeldolgozás-felhasználók nyilvánvalóan nem fogadnának el.

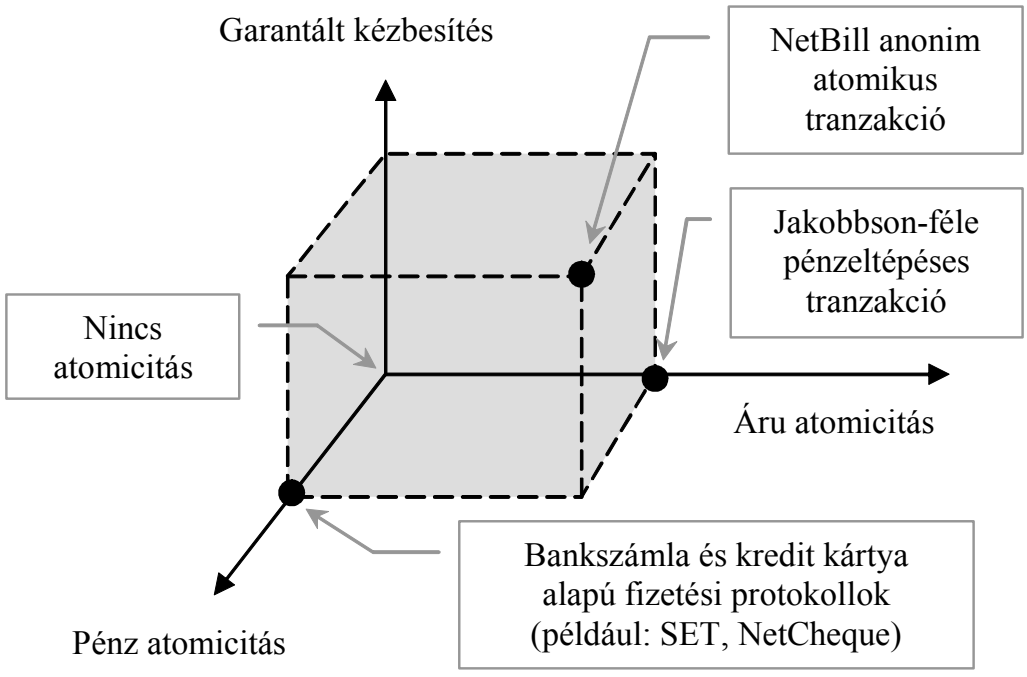
A történet az elektronikus fizetési protokollok esetén azonban egészen más. A publikált protokollok nagy része nem atomikus. Például ha megszakítom a kommunikációt a

protokoll két résztvevő fele között, akkor gyakran inkonzisztens állapotba juthat a rendszer; pénz vagy elektronikus tokenek keletkezhetnek vagy tűnhetnek el.

Elektronikus fizetőrendszerek esetén nem tételezhető fel egyik résztvevő fél viselkedéséről sem, hogy nem fognak eltérni attól az algoritmustól, amin a tranzakciós atomicitás nyugszik. Az atomikus commitment (elkötelezettség) probléma nemcsak azt jelenti, hogy konzisztens, robosztus, a hibáknak ellenálló végeredményt kell produkálni, hanem beleértendő a minden résztvevő által letagadhatatlan részvétel a tranzakciókban. Mindezen célok eléréséhez ki kell kényszeríteni a tranzakció kommitálását, ha bizonyos résztvevők bizonyos monetáris egységeket megkapnak, de a tranzakció egyébként abortált.

[Tan96] egy olyan módszert demonstrál, amellyel fenti tulajdonságú protokoll építhető. Elektronikus check és credit card debit rendszerekre is alkalmazható a módszerük. Az írásban bemutatott VAC (Verifiable Atomic Commitment) általuk megfogalmazott mind a négy követelményének teljesítése további kutatást igényel.

A kutatók [Tyg96a] [Tyg96b] [ST96] az atomicitás három szintjét különítik el.



5. ábra: Atomicitási szintek

3.17.1. Pénz atomicitás (money atomicity)

Az érték olyan módon jut el egyik féltől a másikig, hogy semmilyen körülmények között nem keletkezhet vagy semmisülhet meg érték. Ez az alapszintű atomicitás, amit minden elektronikus kereskedelmi protokollnak elvben teljesítenie kellene.

3.17.2. Áru atomicitás (goods atomicity)

Az áru-atomikus protokollok amellett, hogy pénz-atomikusak, garantálják az eljuttatott pénzért az áru megérkezését is. Vagyis ha valaki áru-atomikus protokollok segítségével vesz egy árut, akkor azt akkor és csak akkor kapja meg, ha fizetett is érte. Ez egy olyan fontos tulajdonság, amit minden információs áruk kereskedésére is használt elektronikus kereskedelmi protokollnak teljesítenie kellene, de egyéb esetekben is nagyon kívánatos lehet.

3.17.3. Garantált kézbesítés (certified delivery)

A garantált kézbesítésű protokollok olyan pénz- és áru-atomikus protokollok, amelyeknél mind a kereskedő, mind a vásárló bizonyítani tudja, hogy pontosan mely áruk kézbesítődtek. Ez akkor kap fontos szerepet, ha a kereskedő vagy a vásárló megbízhatatlan, márpedig ez mindkét esetben feltételezhető.

Az atomicitásra koncentráló kutatók ([Tyg96a] [Tyg96b] [Cox94]) által megalkotott NetBill elnevezésű rendszer kiugró kivétel az eddigi rendszerek között, mert magas fokú atomicitással rendelkezik. Egy külön masters tézis [Cox94] foglalkozik a rendszer privacy aspektusaival, a publikáció középpontjában a privacy és az anonimitás áll.

Az e-commerce protokollok legfontosabb fázisát a fizetési protokollok jelentik, elosztott természetük miatt a résztvevő felekkel szemben magas szintű követelményeket támasztanak. Mivel az alkalmazási logikája ezeknek a megközelítéseknek központilag nem definiált, de minden résztvevő felé el van osztva, a résztvevő példányokkal szemben is magas követelmények fogalmazódnak meg. Több publikáció ezt veszi jobban szemügyre, és ezzel kapcsolatban magas szintű atomicitást és bizonyíthatóságot próbál elérni [SPS99a] [SPS99b] [SP99].

Az általam említett sémák csak magjául szolgálhatnak olyan teljesen kidolgozott pénzrendszereknek, amelyekben a második és a harmadik szintű atomicitás teljes egészében implementálható, azonban ehhez a rendszer tervezése során végig szem előtt kellene tartani az atomicitásból fakadó elvárásokat. Ebben a kérdéskörben nagyon sok a pótolnivaló.

3.18. Kihívás-jelentéstan (challenge semantics)

Egy érme kihívás-jelentéstana [Jak95] [JY96] [Jak97] (challenge semantics) a kihívás bizonyos bitjeihez különféle jelentéseket rendel, ezáltal leírja az érme funkcionalitását. Miután elköltenek egy érmét, utána már nem lehet megváltoztatni az érme kihívás-jelentéstanát.

Ezzel a technikával olyan eszközhöz jutunk, aminek segítségével egy alaprendszert moduláris kiterjesztések széles skálájával lehet kibővíteni. Az ötlet alapján a funkcionalitás kiterjeszthető, ha a kihíváshoz használt bitek bizonyos részei a fizetés jelentését reprezentálják, ill. módosítják. Például egy érméből származó rész-érmét (osztható érmés rendszerek) jelentenek, vagy eseményvezérelt fizetéseket vezérelnek; meghatározhatják, hogy mely körülmények között legyen az érme tárolható;, más bitek beállításával pedig a megcélzott boltot lehet kijelölni. A kihívás-jelentéstan kiválóan használható a pénzeltépéses technika megvalósításához is (3.18.1. fejezet), vagy Jakobsson-féle oszthatóság implementálásához (3.19.3. fejezet).

A kihívás-jelentéstan használata az alaprendszer biztonságát önmagában nem befolyásolja.

3.18.1. Pénzeltépés a fair csere érdekében

A fizetőeszközök árura vagy szolgáltatásra való fair cseréje egy olyan csere, ahol egyik fél sem tudja megkapni a kívánt dolgot, anélkül, hogy az általa felajánlott dolgot átadná. Ha vásárolunk egy liter tejet az ABC-ben, akkor nem tudjuk megkapni a tejet fizetés nélkül, de az eladó se szerezheti meg a pénzünket anélkül, hogy ne adná oda a tejet. Ebben a szituációban nincs probléma a bizalommal, hiszen mindkét fél fizikailag is jelen van. Azonban ha hívnánk egy taxit, megkérnénk, hogy vásároljon bizonyos árukat nekünk, majd térjen velük vissza, akkor bizony már fontos a bizalom: a taxisofőr nem szeretne úgy vásárolni dolgokat, hogy előtte nem fizetjük ki, de mi meg nem szeretnénk fizetni neki, mert nem szeretnénk megkockáztatni, hogy esetleg nem is jön vissza. Mondjuk azt, hogy a taxisofőr fizetsége 100 dollár lenne. Az, hogy az összeg felét az elmenetel előtt kapja meg, a másik felét a visszatérése után, nem oldaná meg a problémát. Azonban ha félbetépjük a 100 dolláros bankjegyet, és a másik felét csak visszatérés után adjuk oda, akkor ez megoldás lehet. Sem mi, sem a taxis nem tudja használni a 100 dolláros felét, mert az értéktelen, de miután visszatért és megkapja a másik felét, akkor összeragaszthatja őket, és használhatja. Ha aggódunk amiatt, hogy a taxisofőr esetleg „csak úgy” nem jön vissza, és így 100 dollár kárunkat okozza, akkor megkívánhatjuk, hogy mindkét fél tépjen el egy-egy

100 dollárost, és adja át egyik felét. Amikor visszatér, átadjuk mindkettő pénz másik felét, és minden rendben van.

A protokoll megőrzi a vevő anonimitását. Az ötlet realizálása részletesen minden pontban teljesíti a fizikai analógiánál elmondottakat. Valójában kétszer elkölthető digitális érméket használnak. Ezek olyan érmék, melyek kétszeri elköltés után még nem fedik fel a tulajdonosok kilétét. Ennek hátránya, hogy a rendszerben kétszer költhető érméket kell mindenhol kezelni, amelyeknek nagyobb a reprezentációjuk (méretük).

[Jak95] először specifikusan a [Fer94] sémát terjeszti ki. Azután mutat egy olyan módszert, aminek segítségével minden olyan protokoll módosítható, ami követ egy bizonyos általános sémát (kihívásokat használnak). Ennél a megoldásnál egy speciális kihívást használnak, melyet a vevő és az eladó közösen állítanak elő. A költség mindössze egy plusz üzenet a protokollban, egy plusz nem költséges függvényhívás mindkét oldalról, és a vevőnél egy kis tárhely a félig elköltött pénzérméknek megfelelő tag-eknek. A megvalósításra még más lehetséges megoldásokat is felvázolnak, mint például megfigyelővel rendelkező TRD eszközök alkalmazását.

A pénzeltépés technika megvalósítására egyszerű módon alkalmazható a kihívás-jelentéstan. Az érme első elköltésénél a vásárló egy olyan kihívást alkalmaz, ahol az egyik bit azt jelenti, hogy a pénz el van tépve, így értéktelen, nem váltható be pénzre a bankban. Az érme másik felét úgy adja oda a vevő, hogy pontosan ugyanolyan kihívást használ fel, mint elsőre, csak az érvénytelenséget jelző bitet a másik állapotba kapcsolja. Ez lesz az a fizetés, amelyre a bank már hajlandó pénzt adni. Ha a második felét nem adja oda soha az eladónak, akkor az üzlet az első felét tudja használni reklamációhoz, és ezáltal megakadályozza, hogy a vásárló azt a felét túlköltés elkerülésével költhesse el ismét.

A kihívás-jelentéstan segítségével megvalósított pénz-eltépéses fair cserével majdnem elérhető a második szintű atomicitás. Tygar és társai felhívták a figyelmet arra, hogy nem ekvivalens, sőt kevesebbet biztosít a második szintű atomicitásnál. Azonban minden séma, amelyben alkalmazható a kihívás-jelentéstan, el tudja érni ezt.

3.18.2. Jakobsson rendszere

Jakobsson rendszere [JY96] [Jak97] az általa feltalált mágikus tintás aláírásokat (3.13.8. fejezet) használ és a kihívás-jelentéstan (3.18. fejezet) technológiáját használja (az utóbbival a rendszer sokoldalúságát növeli). Az általa felállított biztonsági követelmények szigorúak. A mágikus tintás aláírás azon tulajdonsága miatt, miszerint megállapítható, hogy azt valóban a bank állította-e elő, lehetővé válik a bankrablásos támadások elleni

hatékonyabb védekezés. A rendszer olyan kérdésekkel is foglalkozik, hogy esetleges duplaköltés esetén a rendszer többi résztvevője semmiképpen se profitálhasson az eseményből, a látott információ segítségével ne tudja más is még újra elkölteni az érmét.

A mágikus tintás aláírás több résztvevős, elosztott számítású változata is elképzelhető [JY97] [JM99], ebben a biztonság érdekében egyszerre több ombudsman is részt vehet a műveletekben. A rendszer threshold kriptográfiai kiterjesztése tehát több oldalról is támogatva van.

Hátránya a rendszernek, hogy a pénznek lejárati ideje van. A kihívás-jelentéstan segítségével van implementálva, így a lejárati idő olvasható, így véleményem szerint lehetséges, hogy ez az anonimitást veszélyezteti, attól függően, hogy a protokollok során hányan tudhatják meg ezt. Negatívum a hatékonyság szempontjából, hogy az ombudsman nem teljesen passzív, minden pénzkivétnél jelen kell lennie (nem csak mondjuk a regisztrációnál). A rendszer kihívás-jelentéstan segítségével megvalósított oszthatósági kiterjesztése al-érme linkelhető (3.19.3. fejezet).

3.19. Érme oszthatóság és visszajáró

A hagyományos digitális pénzrendszerekben a digitális érmék jól meghatározott címletű pénzt reprezentálnak, melyek csak egészben használhatók fel. Mindenképpen szükség van valamilyen alapvető mechanizmusra, aminek segítségével megoldható, hogy a felhasználó pontosan a kívánt áru értékét adja át az üzletnek.

A legtriviálisabb megoldás bármely érme-alapú sémában alkalmazható módszer, ha a felhasználó sok kis címletű érmét tárol magánál. Persze ez mind tárolási, mind számítási kapacitásban igen költséges, éppen ennek a problémának a leküzdésére dolgozták ki az előbb említett mechanizmusokat. Frankel, Patt, Shamir és Tsiounis analizálta az oszthatóság helyett a többszörös single-term érme használatát. Eszerint ez kis felbonthatósági oszthatóságokra hatékony, de nagyobb felbontásokra megfordul a helyzet, és már érdemes oszthatósági sémát használni. Tsiounis általánosabban is analizálta a témát: több érmét magunknál tartva általgosan gyorsabb a fizetés, de ez pénzkivételnél szűk keresztmetszetté válik számítási és tárolási kapacitásban. A határ a kettő között az oszthatósági pontosságon kívül egy újabb K paramétertől függ, ami azt mutatja, hogy egy pénzkivét után hány tényleges fizetést végzünk; 512 bites modulusra az oszthatós megoldás kisebb, ha $K \cdot \ln\left(\frac{N}{K}\right) \geq 48$, de a kapacitás kisebbé válik, ha $K \cdot \ln\left(\frac{N}{K}\right) > 61$.

Egy másik triviális megközelítés lenne, ha az üzletet visszajáró átadására kérnénk, de ez a pontos érték problémáját az üzletre hárítaná, és az anonimitással is problémák merülnének fel, mert on-line kommunikációt igényelne a bankkal, hogy az a visszajáró anonimitását felfrissíthesse. A privacy-érzékeny felhasználók nem szeretnének a boltoktól visszajárót elfogadni, mert azok az érmék esetleg nyomkövethetők a felhasználó számára nem látható módon.

Elképzelhető megoldás a pénzváltás on-line elvégzése a bankkal vásárlás előtt [BGK95]. A privacy-érzékeny felhasználó azonban nem szeretne a bankkal kapcsolatot teremteni közvetlenül a vásárlás előtt, mert a bank esetleg a bolttal együtt asszociálhatna a felhasználóra (például a felhasználó fizikai helyét beazonosítva a kommunikációs vonal segítségével, vagy a visszajáró és a bolt pénzbetétje közötti időhasonlóságok egybevetésével). A maguktól értetődő megoldások tehát nem megfelelőek.

Egy lehetőség az oszthatóságra, hogy a felhasználó egyszerűen megmondja az elköltendő értéket, belefoglalja egy fizetésnél használt hash számításos kihívásba (hash computed challenge, challenge semantics/electronic checks). Ezek után vagy a fizetés on-line ellenőrződik a bank által a túlköltés megelőzése végett, vagy a trustee jogosult a nyomkövetésre túlköltés esetén.

Talán a legjobb megoldás lehet, ha a felhasználó a birtokában lévő összeget saját belátása szerint beoszthatja. Ilyen, ha a felhasználó a digitális pénzérméit képes felbontani több kisebb címletű érmére. Ezzel majdnem analóg, ha a felhasználónak olyan érméi vannak, amelyeknek a címlete rögzített, azonban a felhasználó ezt több menet során, több vásárlással is költheti el.

Elképzelhető olyan rendszer, ahol működésből vagy felépítésből adódóan (például számláló alapú rendszerek) nem merül fel az oszthatóság problémája. A következőkben olyan eszközöket próbálok bemutatni, amelyekkel kiegészítve az oszthatatlan sémákat, visszajárós vagy osztható sémákat kapunk.

3.19.1. Chaum-féle visszajárós séma

A Chaum [CFN90] által bemutatott on-line típusú rendszerben az érme egy szám, amely a bank privát kulcsai által hatványozva van. Például ha $1/k_1, 1/k_2, 1/k_3, \ldots, 1/k_m$ a bank privát kulcsai egy RSA rendszerben, és az érme 31 egységet ér, ami binárisan 11111, akkor így néz ki: $c = f(n)^{1/k_1 * 1/k_2 * 1/k_3 * 1/k_4 * 1/k_5}$. Az érme leértékeléséhez vagy egy részének elköltéséhez a megfelelő nyilvános kulcsok általi hatványozására van szükség. A mi példánkban, ha el

szeretnénk költeni 25 egységet ($25_{10} = 11001_2$), akkor a k_2-edik és a k_3-adik hatványra emeljük: $c^{k_2 * k_3} = f(n)^{1/k_1 * 1/k_4 * 1/k_5}$, ami 25 egységet ér.

Ebben a rendszerben, ha a vásárló egy fizetést eszközöl, akkor elküldi a banknak a vásárlás értékére leértékelt érmét (d a fizetés bináris értékeinek megfelelő k_i-k szorzata). Ha a pénzváltás csak a vásárló miatt van, akkor a bank egy új érmét állít ki a felhasználónak. A vásárló, hogy felváltassa a pénzt a bankkal, egy „vakolt" m értéket küld, ami az új érme alapja lesz. Amikor visszaadja az érmét a bank, akkor „vakolva" van a bank által $f\left(f(n)^{1/c}\right)$-vel. Ez az érték csak akkor számítható ki a vásárló számára, ha az eredetileg fizetésre használt érme értéke egyenlő volt a fizetendő összeggel és az igényelt felváltandó összeggel, vagyis $f(n)^{1/d * 1/c}$. Ez megakadályozza a felhasználót abban, hogy több visszajárót követeljen, mint amennyi járna neki.

Egy olyan módszert is tartalmaz a rendszer, amivel érmék értékét egy másikba lehet átvinni. Ez azért szükséges, mert sok tranzakció után a felhasználónak lehet, hogy sok érméje lesz, de mindegyik csak egy-két egységet ér. Lennie kell egy módszernek, amivel ezek az érmék egy érmébe kombinálhatóak, hogy később azt egy nagyobb fizetéshez lehessen használni. Ez persze csak akkor szükséges, ha fizetésenként csak egyetlen érmét nyújthatunk át az üzletnek, de általában ez a helyzet. Mivel csak a bank tud aláírni visszajáró érméket, ezt a műveletet mindenképpen on-line kell tenni.

Ez a módszer hátránya is egyben. Azon kívül, hogy egy on-line protokoll költségesebb, a privacy-érzékeny felhasználó nem szeretne a bankkal kapcsolatot teremteni közvetlenül a vásárlás előtt, mert könnyen belátható, hogy ekkor a bank esetleg a bolttal együtt következtethetne a felhasználó személyére.

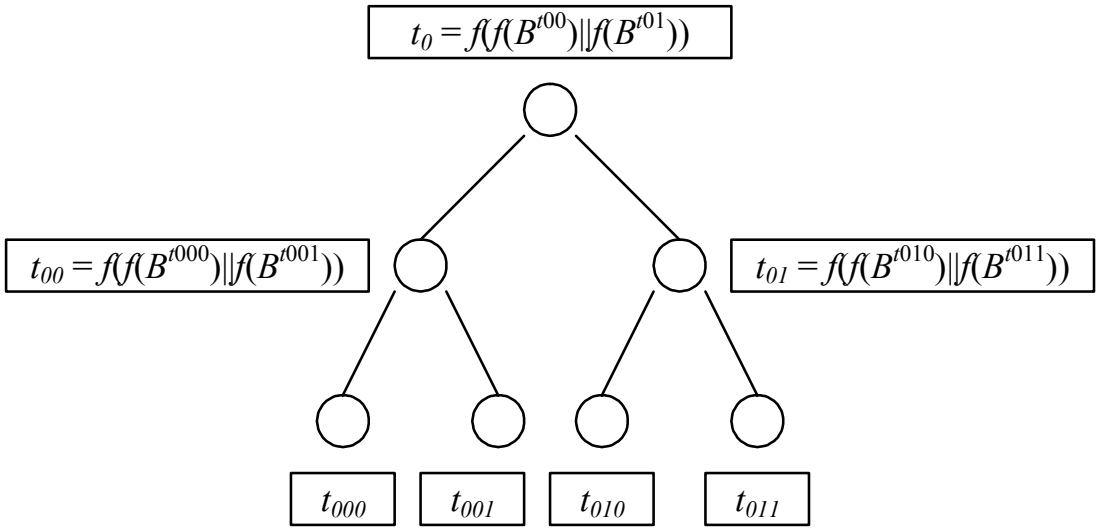
3.19.2. Eng-Okamoto-féle fa struktúrájú oszthatósági séma

Eng és Okamoto [EO95] egy olyan osztható sémát írnak le, amiben egy érmét számos alkalommal el lehet költeni mindaddig, amíg a költések összege el nem éri az érme teljes összegét. Ez a séma off-line módon működhet, és egy fastruktúrára épül. Egy $n = m^2$ értékű érmét egy fa reprezentál, amelynek m szintje és n levele van. A fa gyökere a nulladik szinten található, a fa csomópontja a leendő al-érme jelöltek, amelyek elkölthetőek. Minden l-edik szinten található csomópont 2^{m-l} egység értékű. Két szabálynak mindig teljesülnie kell:

1. egy csomópont nem költhető el többször, és
2. bármely gyökér és levél közötti úton legfeljebb egy csomópont költhető el.

Ha ez a két dolog teljesül, akkor a teljes érme nem használható fel a teljes értékénél nagyobb összegű fizetésekre. Ha azonban a szabályokat megsértik, az érmét kivételező felhasználó kilétének fel kell fedődnie. A publikációban közölt Eng-Okamoto fizetési séma a Ferguson single-term off-line sémájának oszthatósággal módosított változata.

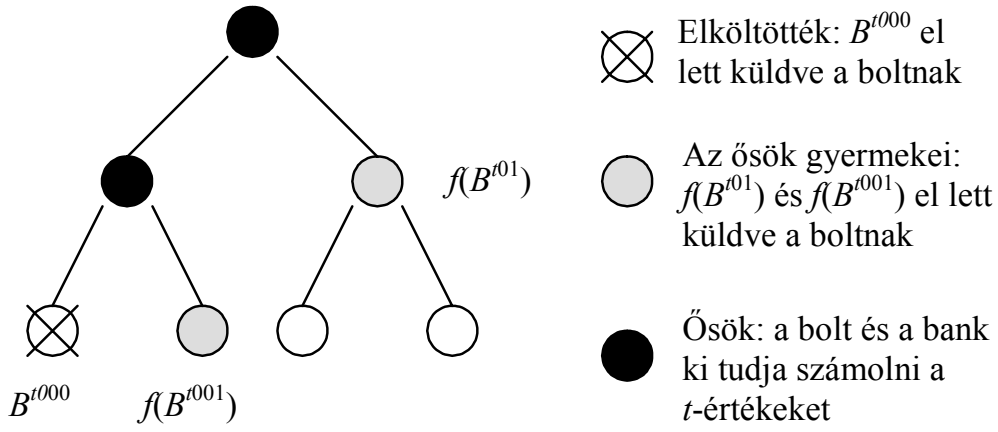
A vásárló először megszerzi a $(CA)^{1/v}$ és $(C^U B)^{1/v}$ aláírásokat a $C = f_c(c)$, $A = f_a(a)$ és $B = f_b(b)$ értékekre a Ferguson sémához hasonlóan, ahol U a felhasználó kiléte. Egy érme számára a fa a következőképpen készül el:



6. ábra: Érmét reprezentáló fa az Eng-Okamoto-féle oszthatóságnál

Minden levélnek van egy hozzárendelt t véletlen szám értéke. Egy belső facsomópont t-értéke a gyermekei t-értékének a függvénye: $t = f(f(B^{t'}) \| f(B^{t''}))$, ahol t' és t'' a jobb és bal gyermek csomópontok t-értékei. Amint elkészült a fa, a vásárló aláírást szerez a banktól a fa gyökerének t-értékére.

A fizetési fázisban, ha a vásárló el szeretne költeni egy csomópontot, akkor elküldi az üzletnek a, b, c-t, a gyökér csomópont t-értékének aláírását, az elköltendő csomóponthoz B^t-t, és az összes őscsomópont testvéréhez tartozó $f(B^t)$ (a gyökér felé vezető úton található csomópontok) értékeket:



7. ábra: Fizetési fázis az Eng-Okamoto-féle oszthatóságnál

Ezekből az üzlet, majd később a bank is képes meghatározni az összes őscsomópont t-értékét, beleértve a gyökerét is, amit a gyökérre adott aláírás hitelességének ellenőrzésére kell használni. Feltételezések alapján ez elégséges bizonyíték az eladónak, hogy az érme érvényes, nem változtatták meg. Az üzlet egy x kihívást küld a felhasználónak. A vásárló $r = t+Ux$ -el és a $(C^r A^x B^t)^{1/v}$ aláírással válaszol, ahol t az elköltött csomópont t-értéke. Az üzlet leellenőrzi, hogy r és az aláírás megfelelő. Ez a fizetési fázis vége.

Ha az első szabályt megsértik, vagyis ugyanazt az al-érmét kétszer is elköltik, akkor ahogy a Ferguson sémában is volt, két r ismert két t-értékhez, így a két egyenletet meg lehet oldani U-ra, felfedve így a csaló kilétét.

Tegyük fel, hogy az első szabály sérül meg, vagyis ugyanazon az útvonalon két csomópontot is elköltenek. Legyen n_1 és n_2 ez a két csomópont, n_1 az n_2 őse. Amikor n_2 elköltődik, akkor az n_2 őseinek testvéreihez tartozó összes $f(B^t)$ értéket megmutatta. Ezekből az értékekből és az n_2 B^t értékéből a bank kiszámolhatja az n_2 összes ősének t-értékét, beleértve n_1-et is. Az n_1 t-értékeiből és az n_1 elköltésének tranzakciójából származó r értékkel megoldhatja az egyenleteket U-ra.

Az a probléma ezzel a sémával, hogy a bank összekapcsolhatja az azonos érméhez tartozó al-érmékkel végzett fizetéseket, mert a gyökér csomópont t értéke minden fizetésnél felfedődik. Noha a pénzkivétekkel nem tudja összefüggésbe hozni egyik al-érmés fizetést sem, az üzletektől a tranzakciókról szerzett protokollon kívüli információkkal lehetségessé válhat a vásárló beazonosítása. A technika úgy tehető összeköthetetlenné, ha megfelelő módon zero-knowledge proof-okat is alkalmaznak a protokollban.

3.19.3. Jakobsson oszthatósági megoldása

A Jakobsson által bemutatott megoldás [JY96] [Jak97] érme-oszthatóság típusú, azaz lehetővé teszi, hogy a rendelkezésünkre álló érméket tetszőleges töredékekre osszuk. A megvalósításra a kihívás-jelentéstan (3.18. fejezet) módszerét hívja segítségül. A bank továbbra is úgy fogadja el az érméket, mint eddig, de csak a kihívásban megjelölt összeggel, vagy pedig az érme teljes összegével növeli a bolt bank számláját, attól függően, hogy melyik a kisebb. Túlköltés fordul elő, ha az érmét nagyobb értékek kifizetésére használják, mint amennyi a megfelelő még megengedett mennyiség. Ha V az érme teljes értéke, és v_i az i-edik költésnél átvitt érték, az érme akkor van túlköltve, ha $\sum_{i=1}^{k} v_i > V$, ahol k jelöli, hogy hányszor fizettek eddig az érmével. Ha az érmét túlköltötték, akkor a bank, mint eddig (a Jakobsson rendszerben), megmutatja az Ombudsmannak a megfelelő nyugtákat, aki ezután leellenőrzi, hogy tényleg túlköltésről volt-e szó, és ettől függően részt vesz az érme-nyomkövetési eljárásában. Sajnos ennél a megoldásnál is az al-érmék linkelhetőek egymáshoz.

3.19.4. Brickell-Gemmell-Kravitz oszthatósági séma

[BGK95] egy pénzváltó mechanizmust mutat be, amely megőrzi az anonimitást, és a [BGK95] trustee rendszertől független. A váltópénz protokoll abban az értelemben on-line, hogy a felhasználónak mindenképpen anonim módon kell tudnia kommunikálni egy digitális pénzverdével (coin minting rendszer). Azonban a [Cha90]-ben mutatottakkal ellentétben a rendszernek a pénzváltó tranzakció során nem szükséges ellenőriznie, hogy az érmét nem költötték-e már el. A protokoll a TTP alapú nyomkövetéstől független, és mind feltétel-nélküli anonimitású, mind TTP anonimitású kontextusban alkalmazható.

A bemutatott protokoll egy hagyományos pénzváltási protokoll lépései szerint zajlik. Az U felhasználónak Y dollárja van, de $X < Y$ értékben szeretne vásárolni. Az U fizetési protokollt használva átadja az Y értékű érmét a B banknak, majd ezután megmondja, hogy milyen címletű érmékre van szüksége. A bank leellenőrzi, hogy ezek összege Y-t ad-e ki. A protokoll során használt egyes értékeket újakra cserélnek minden újonnan kivett érme esetén, az anonimitás megőrzése érdekében. Az érmekivétel előtt a felhasználó a TTP-vel is kommunikál, akitől a pénzkivét protokollhoz szükséges információkat kap cserébe, ha a nyomkövetéshez megfelelő adatokat nyújt át. Ezen információkból származtatott adatokkal már lejátszódhat a pénzkivét.

További vizsgálódást igényel az anonimitás bizonyíthatósága. Mint látjuk, ez is egy on-line pénzváltási megoldás. Nem célszerű a bankkal kapcsolatot teremteni közvetlen a vásárlás előtt, mert a bank esetleg a bolttal együtt asszociálhatna a felhasználóra. Már maga a pénzváltás időpontja árulkodó lehet, hiszen ennek alapján leszűkül azoknak a vásárlásoknak a köre, amelyekből az egyik valószínűleg a felhasználó tranzakciója, ugyanis a vásárlást valószínűleg közvetlen a pénzváltás után teszi meg.

[BGK95] még tartalmaz egy nagyon fontos törvényt, miszerint nem lehetséges feltétel nélküli összeköthetetlenségű hatékony OLC oszthatósági sémát konstruálni. Ugyanis ha egyik al-érme sem hozható információelméletileg kapcsolatba egymással, akkor a maximálisan anonim módon elkölthető al-pénzek entrópiájának a teljes pénz entrópiájánál kisebbnek kell lennie. Ezért az egyetlen esély a összeköthetetlen oszthatóságra, ha komplexitás-elméleti értelemben biztosítjuk az anonimitást.

3.19.5. Okamoto [Oka95] és Chan-Frankel-Tsiounis [CFT98] oszthatósági séma

A korábban látott, Crypt'95-ön bemutatott [Oka95] egy hatékony, anonim, de linkelhető off-line digitális pénz séma, ahol $O(\log N)$ költségű számítás szükséges mind a kivételhez, mind a fizetéshez és a betételhez, ahol $N = \frac{\text{pénzérme teljes összege}}{\text{legkisebb érték amire osztható}}$, más néven oszthatósági pontosság. Ez az eredmény aszimptotikusan optimális, amit Okamoto és Yung 1998-ban be is bizonyítottak.

A [CFT98] oszthatóság tekintetében lényegében az [Oka95] fa struktúrájú oszthatóságát alkalmazza, csak mivel maga a fizetési rendszer más elveken nyugszik, ezért más módon lehet bebizonyítani a fával kapcsolatos tulajdonságokat. A [CFT98] hatékonyságban és biztonságban is felülmúlja az [Oka95]-öt.

Az [Oka95] csak akkor hatékony, ha a számlaalapítás ritkán történik. A számlaalapítást arra használja, hogy egy elektronikus jogosítványt (electronic license) készítsen, melynek segítségével később pénzt lehet kivenni. Azonban annak, hogy bizonyos procedúrákat nem hajtunk végre minden kivételnél (a hatékonyság miatt), az az ára, hogy a jogosítványok linkelhetőséghez vezethetnek. [PW92] megmutatta, hogy minél többet használja a felhasználó a jogosítványt, annál valószínűbb, hogy más módszerekkel (jellemzők alapján való korreláció) linkelhetők lesznek a felhasználók által végzett műveletek. A [CFT98] bankszámla alapítása három nagyságrenddel hatékonyabb az [Oka95]-nél, így a funkcionalitást minden pénzkivétnél alkalmazni lehet, nincs linkelhetőség.

A [CFT98] fő előnye az elektronikus jogosítvány készítésében rejlik, ami néhány tucat hatványozással megoldható, míg az [Oka95] több nagyságrenddel többet igényelne. Ezen felül az [Oka95] sémában a hatványozások száma függ az RSA kulcs méretétől, ami a skálázhatóság egyik gátját jelenti. A [CFT98] hatékony marad fizetés közben is, míg az érme mérete 300 byte körül marad 512 bit modulus esetén. Másik előnye, hogy a digitális pénz séma nyomkövető metódusaival kompatibilis marad [CMS96] [DFTY97] [FTY96], így teljes megoldás fejleszthető ki. Az átruházhatóság moduláris módon hozzáadható.

Az [Oka95]-höz hasonlóan a [CFT98] biztonsági modellje a [FY93]-on alapuló formális modellen nyugszik. Árnyalatnyival erősebb feltételeket teljesít ennek alapján a rendszer, mint az [Oka95]. A tárolási, számítási és kommunikációs költségei a sémának minimálisak, az első hatékony anonim, off-line digitális pénzt eredményezve. Két érdekes nyitott kérdés a rendszer biztonságának bizonyítottabb feltételezésekre helyezése, és olyan módszer találása, amely megtöri az érme al-érméi közötti linkelhetőséget.

3.19.6. Nakanishi-Haruna-Sugiyama [NHS99] oszthatósági séma

Az [NHS99] séma ún. elektronikus kupon (coupon, szelvény) protokollokkal dolgozik, amelyeknél a kivett érme sok al-érmére osztható, és amelyeknek a névértéke előre rögzített. Az eredeti érmét jegynek (ticket), az al-érméket al-jegyeknek hívják. Az al-érméknek fix névértéke van, a névértékek összege az érme értékével egyenlő. Az eredeti érmét nem lehet elkölteni, csak az al-érméket. Egy e-kupon protokollban a fizetés úgy valósul meg, hogy a kivett jegynek a tulajdonosa bizonyítódik (ami a bank digitális aláírása), anélkül, hogy maga a jegy felfedődne. Ezen felül a túlköltés érzékelése érdekében a vevő kényszerítve van, hogy azonos értékű érméket küldjön, akkor és csak akkor, ha a vevő ugyanazokat az al-érméket használja (akkor és csak akkor linkelt a két fizetés).

Az [NHS99]-et megelőző osztható kupon protokolloknál az egy jegyhez tartozó al-jegyek linkelhetőek voltak, ami teljes de-anonimizációhoz vezethetett. [NHS99]-ben egy olyan elektronikus kupon protokollt közölnek, ahol az al-kuponok nem linkelhetők, ráadásképpen az anonimitás visszavonására is van lehetőség.

Az [OO98] kupon sémájában a fizetés másolata tartalmazta magát a kivételezett érmét, ami egy, az érme érvényességét bizonyító digitális aláírás. Így, az egy érméből származó al-érmék fizetési másolatai linkelhetők, a különböző érméből származók összeköthetetlenek. Hasonlóan az itt bemutatott többi oszthatósági sémában is az al-érmék linkelhetők.

Az [NHS99]-ben bemutatott protokoll [CSM97] csoport-aláírásokat (3.14. fejezet) használ. A [CMS97] sémában a csoport a csoport manager által kibocsátott hamisíthatatlan tanúsítványt birtokló tagokból áll. Ha a tanúsítványt jegyként használják és a csoport-aláírás a fizetés másolataként szolgál, akkor a következő igaz a csoport-aláírás tulajdonságai miatt:

Az első tulajdonság biztosítja, hogy a vevőnek van jegye, a második tulajdonság biztosítja, hogy a fizetés anonim és összeköthetetlen, a harmadik tulajdonság pedig biztosítja, hogy a túlköltő vevő azonosítható legyen, ha a túlköltés észrevehető. Azonban ha a fizetés másolata csak a csoport-aláírás, akkor a túlköltés észrevétele lehetetlen, mert az al-érme különböző elköltései nem linkelhetők. Ezért [NHS99] protokolljában a fizetés másolata a csoport-aláírásból és egy olyan értékből áll, ami akkor és csak akkor egyenlő két fizetés esetén, ha a vevő ugyanazt az al-jegyet használja. Így a túlköltés az elköltések érvényes másolataival detektálható.

Az elrablásos támadás ellen úgy védekezik a rendszer, hogy zsarolás hatására olyan módba képes átmenni, hogy minden fizetést egy trustee-nál on-line verifikálni kell. A bemutatott sémában bármely érték fizetése $O(N)$ számítást igényel (N a felbonthatósági pontosság). A [CFT98]-ban $O(\log N)$ -eset mutatnak, de abban az egy érméből származó al-érme költések linkelhetőek. Az $O(\log N)$ -es nem linkelhető protokoll még nyitott probléma.

3.19.7. Nakanishi-Sugiyama [NS99] oszthatósági séma

[Oka95] és [CFT98] $O(\log N)$ hatékonyságú, de al-érme linkelhető. [NHS99] elektronikus kupon protokollja linkelhetetlen, de $O(N)$ költségű. Belátható, hogy N szerepe a számítási komplexitásban nagy lehet. 1000 dolláros érme és egy cent legkisebb oszthatósági érték esetén $N\,2^{17}$-es nagyságrendű. Egy rendszer már hatékony lehetne $O(poly(\log N))$ esetén.

[NS99] $O((\log N)^2)$ költségű mindenféle számítási tekintetben. Az előbbi [NHS99] e-kupon rendszeren alapul. [NS99] osztható digitális pénzrendszerben a bináris fa megközelítést adaptálják az $O(poly(\log N))$ számítási komplexitás realizálására ([Oka95]-ben és [CFTY98]-ban is bináris fa van). Ebben a megközelítésben egy kivett érmének egy bináris fája van, amiben a gyökér az érme értékét jelenti, és a gyerek csomópontok a szülő csomópontok értékének a felét jelentik. Az érme tulajdonlásának bizonyítása mellett az e-kupon rendszerhez hasonlóan a vevő kényszerítve van arra, hogy olyan érméket küldjön, amelyek akkor és csak akkor vannak linkelve, ha a gyermek-szülő kapcsolat pontjai fizetésre voltak használva, vagy ugyanazt a csomópontot többször használták fizetésre, ami a túlköltést jelenti.

3.20. Átadhatóság technikák

3.20.1. Eng-Okamoto-féle [EO95] átadhatóság

Eng és Okamoto a sémájukba bevették azt a képességet, hogy egy személy egy másik személynek bank közreműködése nélkül adhasson át érméket. Mielőtt a vásárló kivételez egy érmét, először egy engedélyt kell kérnie. Ez az engedély információkat hordoz a vásárló kilétével kapcsolatban. Az engedély szükséges a pénzkivéthez és az elköltéshez. Egy engedéllyel kivett pénz csak ugyanazzal az engedéllyel költhető el.

Amikor az egyik fél, mondjuk Alice átküld egy érmét egy másik félnek, mondjuk Bobnak, Alice csatol egy tanúsítványt a Bobhoz való átküldésről, majd ugyanolyan fizetési protokollban vesz részt, mint amilyen a vásárló és az üzlet között is zajlik. Amikor Bob elkölti az érmét egy boltban, akkor elküldi az érmét, majd az Alice által adott tanúsítványt és nyugtát is. Habár az engedély nem ugyanaz, mint amivel a pénzt kivették, de a bolt ellenőrizheti az Alice és Bob között lezajlott átvitel nyugtáját, Alice tanúsítványát, és a tanúsítvánnyal az érmét is ellenőrizheti. Ezután Bob és a bolt a szokásos fizetési protokollban vesz részt Bob engedélyének használatával.

Mivel a felhasználó kiléte az engedélybe be van ágyazva, függetlenül attól, hogy ki vette ki a pénzt a bankból, az a személy, aki esetleg másodszor költi el, azonosítható lesz. Az átvitel tanúsítvány pedig garantálja, hogy Bob-on kívül Alice kiléte is kiderüljön.

3.20.2. Van Antwerpen átadhatósági séma

Van egy általános, Antwerpen nevével fémjelzett módszer [Ant90], amelynek segítségével az üzletek pénzt adhatnak át más kereskedőknek. A módszer megőrzi az üzletek anonimitását, minden anonim off-line pénzre. Az sem számít, hogy a rendszer pénzérme vagy számláló alapú.

Lényege: az üzlet kap egy „üres” (0 értékű) „vakolt” érmét a banktól, és beágyazza ezt a felhasználónak küldött random kihívás hash-ébe (pontos fizetések érdekében osztható üres érmék is kaphatók). Ezután az üzlet átadhatja a felhasználótól kapott fizetést egy másik kereskedőnek az üres érme „elköltésével” (egy fizetési protokollban vesz részt vásárlóként). Az üzletnek csak kapcsolatot kell létesítenie a bankkal (off-line módon), hogy megkaphassa az üres érméket. Az még jövőbeli kutatást igényel, hogy olyan algoritmust találjanak, amellyel egy kivét segítségével több üres érméhez jutunk, és gyorsabb, mint több egymás utáni egy-érmés pénzkivét.

Hátrány, hogy a számítási és a tárolási költség az érme átadásainak számával nő. Ez k darab átadás esetén $2k$ db aláírás ellenőrzést, azaz nagyjából $\frac{2}{3}k$ RSA teljes hatványozást jelent. Sajnos ez egy praktikus, PDA-t vagy smart card-ot használó rendszerben megterhelő (főleg az aláírás-ellenőrzés számításigénye, de a méretnövekedés sem elhanyagolható). Chaum és Pedersen megmutatta [CP93a], hogy a költségek elkerülhetetlenek, és ez a megközelítés aszimptotikusan optimális. A rendszer biztonságának elfogadottabb és bizonyítottabb feltételezésekre helyezése még várat magára.

3.21. Elvesztésállóság (loss-tolerance)

Az elvesztésállóság [WP90] [PW95] [PW97] annyit jelent, hogy ha a vásárló pénze elveszik, ellopják, megsérül, vagy meghibásodik, akkor visszakapja a pénzét.

Elvárások az elvesztésállósággal szemben:

1. A bank biztonsága. Csaló felhasználók nem tehetnek szert pénzre jogtalanul.
2. Azon felhasználók biztonsága, akik nem vesztik el az eszközüket. E felhasználók semmiképpen sem veszthetnek pénzt a technika alkalmazása miatt.
3. Elvesztés-tolerancia: az elvesztett elektronikus pénztárca tulajdonosához visszakerül a pénze egy adott időintervallum letelte után
    a) Erős elvesztésállóságról beszélünk, ha ez olymódon garantált, hogy közben a felhasználónak nem kell megbíznia a rendszerben résztvevő többi félben (bank, kereskedők).
    b) A gyenge elvesztésállóság csak akkor garantált, ha a bank „hűséges", jóhiszemű módon viselkedik.
4. Azon felhasználók követhetetlensége, akik nem vesztik el az eszközüket. E felhasználók privacy-jét semmiképpen sem veszélyeztetheti a technika alkalmazása.
5. Tárcájukat elvesztett felhasználók részleges követhetetlensége. Technikai okok miatt a tárcájukat elvesztett felhasználók fizetéseit nyomkövetni kell. Általában csak az utolsó pénzkivét és az elvesztés ideje közötti fizetéseknél van szükség erre.

Az alábbiakban a [WP90]-ben tárgyalt elvesztésállóságot szeretném bemutatni. A szerzők csak számláló alapú rendszerre vizsgálják kérdést, elvesztés ellen csak az elektronikus

tárcákat védik, de nem védik az elektronikus pénztárgépeket (POS terminálok), vagy a banki gépeket.

Az elvesztő privacy-je az elvesztés körüli néhány tranzakció erejéig felfüggesztődik, illetve nyomkövetődik. Az elektronikus pénztárcák elvesztésállóságának az elosztott visszanyerésen (distributed recovery) kell alapulnia. Az elvesztést vagy az ellopást nem lehet belső hibatűrő (fault-tolerant) mechanizmusokkal vagy külső intézkedésekkel kezelni (például a háromból két tárca megoldás impraktikusnak tűnik, ráadásul az ember valószínűleg egyszerre mind a hármat elvesztené).

Speciális a helyzet az átadható digitális pénz esetén; ekkor bizonyos elvárásokat gyengíteni kell. Lehetetlen például akkor előkeríteni az elvesztett pénzt, ha azt egyik tárcáról a másikra továbbították, majd mind a két tárca elveszett. Átadhatatlan (non-transferable) tulajdonsággal rendelkező, érme-alapú rendszerek esetén az elosztott visszanyerés a következő lehet:

Időről időre, általában pénzkivétek után a tárcában tárolt információról másolatot kell készíteni, archiválni kell. Az érme-alapú rendszereknél ez a backup információ aláírt érméket tartalmaz (a vak aláírás protokoll utáni transzformált alakban). Mivel ez nagyon érzékeny adat, ezért a felhasználónál kell maradnia, rejtjelezett formában. Az előbbi azt jelenti, hogy a felhasználónak egy másik eszközre van szüksége, az utóbbi pedig kulcs-menedzsmentet igényel.

Elvesztés után a pénztárca tulajdonosa kapcsolatba lép a bankkal, és részt vesznek egy visszakövetelés (reclaiming) protokollban. A visszanyerés során szükség van a bankra, hogy megakadályozzuk az olyan csaló felhasználókat a backup információk használatában, akik el sem vesztették az eszközüket, és kétszer akarják elkölteni a pénzüket. A pénztárca tulajdonosa is szükséges, hogy a backup adatokat szolgáltassa, vagy segítse azokat kirejtjelezni.

A legtöbb esetben a felhasználók a backup információban szereplő pénzek egy részét az elvesztés pillanatában már elköltötték. Az adott szituációt pontosan csak az elektronikus pénztárgépek segítségével lehet felmérni. A felhasználó az összes olyan pénzt megkapja, amelyeket nem ő költött el, és még nem tették be a bankba. Az ennek megfelelő protokoll részleteket „elhelyezés”-nek (settling) nevezik. A visszakövetelés és az elhelyezés együtt a „visszanyerés” (recovery). Meg kell akadályozni, hogy ha esetleg a felhasználó rosszhiszemű módon jelentett elvesztést, a visszakövetelés procedúra után megpróbáljon érméket elkölteni.

A backup történhet saját eszközre (smart card), vagy más eszközére. A saját eszköz tipikusan egy másik smart card lehet, míg más eszközére jó példa lehet a felhasználó bankja által biztonságos módon tárolt információ. Saját eszköz esetén az archiválás műveletének a felhasználó explicit kérésére kell megtörténnie, ekkor egy erre szolgáló „backup" tranzakció zajlik le. Az archiválás egyszerű esetben lehet az előzőt felülíró típusú, de elképzelhető inkrementális backup, vagy más mechanizmus is. Banki backup esetén a műveletnek automatikusan meg kell történnie minden pénzkivét után.

A pénz lejárata vagy érme-feketelistázás, vagy pedig lejárattal bíró érmék segítségével valósítható meg. Az esetleges tolvaj rosszindulatú tevékenységét maga az elektronikus tárca felhasználó-hitelesítési eljárása akadályozhatja meg, ami általában PIN szám alapú védelem. PIN kódból eleve kettőt is célszerű használni, egyet a pénzkivétekhez, és egyet fizetésekhez. Mindkettőt gondosan kell kezelni.

A leírtak erős elvesztésállóságot eredményeznek. A vázolt megoldás idealista, a teljes implementációhoz legalább 1-es szintű atomicitás is szükséges.

Az igények kielégítése érdekében több dologgal meg kell barátkozni:

1. Az elvesztett digitális pénz lejár: egy adott idő lejárta után garantálni kell, hogy elkölthetetlen legyen. Ez protokoll és szinkronizációs feladat.
2. A technika nem lehet teljesen transzparens, a felhasználónak minimum követelményként el kell mentenie bizonyos információkat, amelyeket elvesztés után vissza kell töltenie.
3. A backup információ kockázatot jelent a felhasználó privacy-jére (követhetetlenség) nézve, főleg a backup TRD nélküli megoldásoknál.

Azonban más biztonsági tulajdonságok nem gyengülnek, és a rendszer hatékonysága nem csökken észrevehető mértékben.

4. Egy ideális digitális pénz séma tulajdonságai

Az irodalomban több mint 30 féle tulajdonságot definiálnak elektronikus fizetési rendszerek jellemzésére. Látni fogjuk, hogy sok ezek közül szorosan összefügg, és egy tulajdonságban összegezhető. Az alábbiakban sorra veszem a tulajdonságokat, először fontossági sorrendben a leglényegesebbeket, amelyekkel egy ideális digitális pénzrendszernek is mindenképpen rendelkeznie kell, majd más olyan kívánatos tulajdonságokat is, amelyeknek a praktikusság miatt szintén egy ideális rendszer részét kell képezniük.

4.1. Biztonság (Security)

A legfontosabb tulajdonság a biztonság. A később leírt bizalmasság, hitelesség, integritás és letagadhatatlanság tulajdonságok maguktól értetődőek, és részei a sémák kriptográfiai protokolljának, így az ideális digitális pénzrendszerének is. A bizalmasságot a kriptográfiai technikák és rejtjelezések explicit módon illetve mellékhatásként biztosítják. Az integritást az anonimitásért felelős kriptográfiai technikák biztosítják. Ha az ideális séma digitális aláírást is használ, a letagadhatatlanság implicit módon biztosítva van, ellenkező esetben bizonyítottnak kell lennie.

Ezeknek a tulajdonságoknak nem elég pusztán a megléte, az is fontos, hogy milyen kriptográfiai és matematikai technológiákkal éri el a séma a biztonságot, mivel védekezik a később bemutatott logikai támadások ellen. A bűncselekmények ellen védő kriptográfiai technikák alapvető jellemzői a bennük alkalmazott nevezetes kriptográfiai protokollok típusa. Ezeknél tudható, hogy mely feladatok megoldásának nehézségére vezethető vissza feltörésük nehézsége. Fontos, hogy egy ideális digitális pénzrendszerben teljes egészében bizonyítottnak kell lenniük a biztonság egyes aspektusainak. Legyünk telhetetlenek, és azt is kívánjuk meg, hogy mindez formális módszerekkel is igazolva legyen. Az ideális rendszerben a védelem olyan kriptográfiai, számításelméleti és információelméleti problémák nehézségére vezethető vissza, amelyeket a kriptográfusok széles körben elfogadnak és nehéznek tartanak.

A legfontosabb jellemző tehát a rendszer biztonsága, amely sok altulajdonságot foglal magába. A biztonság mögött a következő tulajdonságokat szokták számba venni, ezeket egy ideális rendszernek mindenképpen teljesítenie kell.

4.1.1. Bizalmasság (Confidentality)

Egyrészt külső szemlélők nem képesek megfigyelni a résztvevő felek között végbemenő tranzakciókat. Másrészt a tranzakciókban résztvevő felek számára az információhoz való hozzáférés a szerepüknek megfelelően korlátozva van. Az elsőt a kriptográfiai technikák és rejtjelezések biztosítják; a későbbit, amelyet néhányan az integritás tulajdonságba sorolnak, az anonimitás illetve az azzal járó kriptográfiai technikák biztosítanak.

4.1.2. Hitelesség, hitelesítés (Authentication)

A sémában szinte minden mozzanatban implicit vagy explicit módon ott kell lennie a hitelesítésnek. A kommunikáció során a hitelesség kölcsönösen biztosítja mindegyik felet,

hogy a tranzakcióban résztvevő többi félnek megfelelő, érvényes az identitása. A hitelesség biztosíthat egy résztvevő felet arról, hogy egy entitás vagy információ hiteles:

- a kereskedőnek tudnia kell ellenőrizni, hogy a digitális pénz érvényes, valódi;
- a banknak tudnia kell megbizonyosodni arról, hogy a tranzakció hitelesített felek között ment végbe;
- léteznie kell olyan eljárásnak, amellyel leellenőrizhető a kereskedő bankja és bankszámlája, a vevő bankja és bankszámlája.

4.1.3. Integritás (Integrity)

Biztosítja, hogy a tranzakciót nem tudja megváltoztatni olyan résztvevő, aki közvetlenül nem vesz részt az ügyletben. Sőt, ezen felül a résztvevő felek is csak jól meghatározott paramétereket módosíthatnak a tranzakció lefolyása során (például a kereskedő nem írhatja át a vételárat). Ez tehát egy külső és belső védelmet jelent a manipulációk ellen.

Gyakori az előzőekkel majdnem ekvivalens megfogalmazása az integritásnak, miszerint nem adható hozzá monetáris érték a rendszerhez és nem vonható ki a rendszerből monetáris érték nem szabályos úton. Ez magában foglalja a hamisításnak, dupla költésnek és egyéb bűncselekményeknek való ellenállást. Az integritást egyrészt a rendszer kriptográfiai technikákkal elért biztonsági tulajdonságai, másrészt az atomicitás biztosítja. Gyakran az integritás tulajdonság alatt bizalmassági követelményeket is értenek: titkos vagy privát információ nem férhető hozzá a rendszerben explicit engedély nélkül.

4.1.4. Letagadhatatlanság (Non-Repudiation)

Miután érvényesen lezajlott egy tranzakció, egyik résztvevő sem tudja letagadni annak végbemenetelét. A letagadás elleni bizonyítási eljárást csak a kifejezetten ezzel foglalkozó publikációknál szokták kidolgozni, a többi esetben megelégszenek azzal a ténnyel, hogy elvégezhető. Fontos szerepet kap vitás esetekben az atomicitás is. Külön publikációk foglalkoznak azzal, hogy hogyan lehet gördülékenyen megoldani a vitás esetek feloldását (dispute resolution), és hogyan alkothatók olyan rendszerek, amelyekben a feloldás minél automatikusabban, emberi beavatkozás nélkül megy végbe.

Egy ideális rendszernél elvárjuk, hogy a letagadás kérdésköre is teljes körűen tárgyalva és bizonyítva legyen. A viták feloldása automatikusan tudjon végbe menni. Mivel egy ideális rendszer garantált kézbesítés (harmadik szintű) atomicitással rendelkezik, ezért szerencsére ez a tulajdonság segít megvalósítani a vitafeloldást.

4.1.5. Engedélyezés (Authorization)

A rendszer lehetőséget biztosít arra, hogy résztvevő felek engedélyezhessék, jóváhagyhassák az elektronikus tranzakciót. Ez egy olyan lépés, amit a való életben is sokszor tapasztalunk, főleg nagy értékű vásárlás esetén. A protokollokat nem szükséges módosítani, csak arra kell figyelni a teljes rendszer megvalósítása során, hogy a vásárló láthasson egy számlát (lehet elektronikus is) a tranzakcióról, és ezt jóváhagyhassa. A tranzakció elvetése valamilyen rendszeren kívül származó rendellenesség esetén jön szóba, ami megjelenik a számlán (például egy bevásárlóközpontban a termékre az akciós ára helyett a normál árát számlázzák). A rendszert célszerűen úgy kell felépíteni, hogy ez még a fizetési tranzakció előtt kiderüljön, így nem szükséges új fázis felvétele a rendszerben (egy fizetés-visszavonási fázis). Csak oda kell figyelni a rendszer tervezése során ezekre a kívülről fakadó problémákra.

4.1.6. Visszaigazolás (Confirmation)

Mind a kereskedőnek, mind a vásárlónak kapnia kell egy igazolást arról, hogy a tranzakció végbement, ezáltal mindketten tudják, hogy a pénz gazdát cserélt. Adott esetben ezek az igazolások lehetnek a bizonyítékok arra, hogy a fizetés megtörtént.

A jelenlegi kredit-kártyás sémáknál az engedélyezés és a visszaigazolás is létező funkciók. Jogos az elvárás, hogy a digitális pénz is biztosítsa ezeket. Habár nagyon fontos ez a két tulajdonság, de mivel nem szerves részei a sémák magjának, és a rendszerekhez hozzáadhatók, ezért általában nem foglalkoznak vele a kutatók. Egy ideális rendszernél azonban szükséges, hogy ezek a kérdések is teljes körűen vizsgáltak és tisztázottak legyenek.

4.1.7. Rendelkezésre állás (Availability), Megbízhatóság (Reliability)

Egy ideális elektronikus fizetési rendszernek folyamatosan használhatónak kell lennie. A vásárló akkor és ott szeretne fizetni vagy pénzt kapni, ahol számára szükséges. Noha ez a tulajdonság is fontos része a tágabb értelemben vett biztonságnak, elsősorban szervezési eszközökkel biztosítható: dual host-ok, redundáns erőforrások (szerverek, kommunikációs vonalak, stb.). Az ideális séma annyit segíthet a magas rendelkezésre állás elérésében, hogy megpróbálja minimalizálni a DoS (Denial of Service) támadások kockázatát, melyek a rendelkezésre állást sértik. Rendszer-szerkezetileg az segíthetne, ha nem lenne olyan központi szerver, ahol számítások koncentrálódnak és ily módon a rendszer gyenge pontját képezik. Sajnos ez nem megoldható, a védekezés szintén inkább szervezéssel oldható meg:

például a fent említett módszerek, redundáns és backup szerverek alkalmazása, különböző bankfiókokban való elhelyezése. A DoS elleni támadást nehezebbé teszi, ha a bankra kevesebb számítási és tárolási munka hárul tranzakciónként. Ez túlmutat a biztonságon, skálázhatósági és hatékonysági követelményeket is jelent. DoS védekezési szempontból legalább ennyire fontosnak bizonyul a protokollok fizikai implementációjának, realizációjának támadhatatlansága is, mert a biztonsági rések kihasználásával a szerver lefagyasztható, ami szintén szolgáltatáskiesést eredményez. Egy ideális rendszer egy ilyen támadásnak ellenáll.

Egyes szakirodalmi művek azt értik megbízhatóság alatt, hogy a fizetés tranzakciónak atominak kell lennie: vagy teljes egészében megtörténik, vagy egyáltalán nem. A hibákból való felépülés stabil tárolást és megbízható visszaállítási mechanizmusokat igényel. Az atomicitás tulajdonság mindezeket magába foglalja.

4.1.8. Ellenállás a logikai támadási lehetőségeknek

Tekintsük a biztonságnak azt az aspektusát, amely a logikai támadásokkal szembeni védelmet és a bűncselekményekkel szembeni ellenállást jelenti. Ahhoz, hogy jobban átláthassuk, hogy ez milyen feltételeket támaszt a sémákkal szemben, érdemes áttekinteni a lehetséges támadásokat. Egy ideális rendszer ezeknek mind ellenáll. Különösen nehéz és nem kielégítően megoldott a bankrablás típusú támadások elleni védekezés.

- Hamisítás (Forgery): A támadók csoportja együttműködik, hogy olyan hamisított pénzösszeget vegyenek ki felhasználók számára, vagy olyan hamisított vásárlásokat vigyenek véghez, amelyek egy becsületes bank számára valódinak tűnnek.
- Túlterhelés (Impersonation): A támadók csoportja egy felhasználót nagyobb összeggel terhel, mint amennyit az valójában elköltött. Ez például úgy lehetséges, hogy a résztvevő felek, közöttük egy kereskedő, duplán vagy még többször próbálnak pénzt betenni egy tranzakció információi alapján.
- Túlköltés (Overspending): Egy felhasználó egy szabályosan kivett összeget magasabb értékkel költ el, mint amekkora az valójában. Túlköltés az is, ha a felhasználó az érvényesen kivett érmével többször is fizet. Ekkor a második és az azutáni fizetési tranzakciók csalások. Dupla költésnek (double spending) nevezik, ha kétszer használja fizetésre az érmét.
- Illegális vásárlások (Illegal purchases): Olyan tranzakciók, amelyek pénzforgalmi szempontból teljesen érvényesek, de a vásárolt áruk természete miatt nem legálisak.

- Pénzmosás (Money laundering): egy vagy több résztvevő fél leplezi a megkérdőjelezhető forrásból származó bevételének forrását úgy, hogy az egy másik üzleti vállalkozás bevételének tűnik. Ez adott esetben illegális pénzmozgatási tranzakció segítségével érhető el. A kivédéshez a rendszernek képesnek kell lennie a fizetések nyomkövetésére, hogy stabil bizonyítékot lehessen felmutatni bűntény felmerülése esetén.
- Zsarolás (Blackmail): Egy támadó arra kényszeríti a felhasználót, hogy vegyen ki pénzt neki oly módon, hogy végül csak a támadó ismerje az érték digitális reprezentációját. Ezt általában úgy érheti el, hogy a felhasználót és esetleg a bankot is egy nem standard protokollban való részvételre kényszeríti. A tökéletes anonim bűntény [SN92] ellen szintén nyomkövetéssel lehet védekezni, azonban ez további problémákat vet fel (3.16. fejezet).
- Bankrablás (Bank robbery): Kétféle támadást különítenek el ilyen néven [JY96] [Jak97]. Az első típusúban az issuer (bankok és más entitások, amelyek kezében van a pénz készítéséhez vagy követéséhez szükséges titkos kulcs) entitástól egy támadó megszerzi a titkos kulcsot, például belső támadással, vagy valamilyen módon kényszeríti erre. A második típusú bankrablásban, amely akkor lehetséges, ha a pénzkivételek „vakolhatóak", a támadó ráveszi az issuer bankot, hogy egy nem standard „vakolt" pénzkivétel protokollban vegyen részt, és így illetéktelenül pénzhez jut. Ezt a típust félrevezetésnek is (blindfolding) nevezik, illetve a két támadást együttesen bankrablásos támadásként emlegetik. Ezek a támadások azért nagyon súlyosak, mert ha az érme hitelessége az issuer aláírás-függvényétől függ csak, akkor praktikusan nem lehetséges az aláíró számára az illegálisan előállított pénzek követése, ezáltal a támadó kilétét nem lehet felfedni.
- Rosszindulatú nyomkövetés (Malicious tracing): Támadás Bankok és Ombudsmanok csoportja által, melynek során törvényes felhatalmazás nélkül nyomkövetnek pénzeket, pénzkivételeket, tranzakciókat. A banknak, mint profitorientált entitásnak érdekében állhat az ügyfeleiről adatokat gyűjteni (hovatovább esetleg más vállalatoknak statisztikákat vagy profilokat értékesíteni). Ennek elkerülése érdekében a követési tranzakciókba, és magába a digitális pénzrendszerbe további résztvevő feleket kell bevenni (Ombudsman, TTP), akik a kérdéses bank irányításán kívül esnek. Ezeket az entitásokat társadalmi érdekképviseleti szervezetek üzemeltethetik, illetve a törvényhozáshoz is tartoznak Ombudsmanok, amelyek érvényes bírói ítélet alapján cselekszenek. Kriptográfiai szempontból több-résztvevős protokollokra és threshold kriptográfiára van szükség.
- Koholt vád (Framing): A támadásban résztvevő felek úgy tüntetik fel, hogy egy felhasználó vagy egy kereskedő részt vett egy adott tranzakcióban, miközben ez

nem igaz. Adott esetben képesek fizetési számlát is generálni, melyet nyomkövetve a becsületes felhasználóhoz vagy kereskedőhöz jutnak el a hatóságok.

- Sikkasztás (Embezzlement): Olyan támadás, melynek során a felhasználó pénzt veszít, mert a bank érvénytelennek tüntet fel egy tranzakciót, vagy csak kevesebb pénzt fogad el, pedig több érvényes érme/érték is rendelkezésére áll a felhasználónak.

1. táblázat: Támadások összegzése

Becsületes / *Támadó*	Felhasználó	Kereskedő	Bank	Trustee	Mindenki
Felhasználó	Zsarolás, Megszemélyesítés	Túlköltés	Hamisítás, Túlköltés, Bankrablás		
Kereskedő	Sikkasztás, Megszemélyesítés	Megszemélyesítés	Hamisítás, Pénzmosás, Bankrablás		Pénzmosás
Bank	Rosszindulatú visszakövetés, Koholt vád, Sikkasztás	Koholt vád, Sikkasztás			
Trustee	Rosszindulatú visszakövetés, Koholt vád				
Támadók csoportja	Támadások variációi	Támadások variációi	Támadások variációi	Támadások variációi	Illegális vásárlások, Pénzmosás, Variációk

4.1.9. A logikai támadási lehetőségekből fakadó követelmények

Hogy mindezek a támadások elkerülhetők legyenek, többek között a következő biztonsági tulajdonságok megléte is szükséges:

- Hamisíthatatlanság (Unforgeability): Csak az arra felhatalmazott entitások képesek érvényes digitális pénzt kibocsátani.
- Megszemélyesíthetetlenség (Impersonation safety): A megszemélyesítés nem lehetséges.
- Túlköltés-érzékelés (Overspending detection).

- Túlköltés-robosztusság (Overspending robustness): Ha több résztvevő fél követ el túlköltést ugyanazon információk (érme információk) felhasználásával, akkor a nyomkövetéssel mindegyikük identitása kideríthető.
- Nyomkövethetőség (Traceability): lehetséges a pénzkivétel- és az érme-nyomkövetés. Opcionális esetben (pénzkivétel, érme) pár összetartozásának eldöntése.
- Visszavonhatóság (Revokability): Gyanús érmék ideiglenesen elkölthetetlenné tehetők, például feketelistás technika segítségével. Egy ideális rendszer esetén pedig követelhetjük, hogy ez ne rontsa a rendszer hatékonyságát.
- Anonimitás (Anonymity)
- Koholt vád lehetetlensége (Framing-freeness)
- Visszaforgathatóság (Refundability): sikkasztásos támadás esetén a kárt elszenvedő áldozat bizonyítani tudja támadást, és legalább az egyik támadó kiléte kiderül.

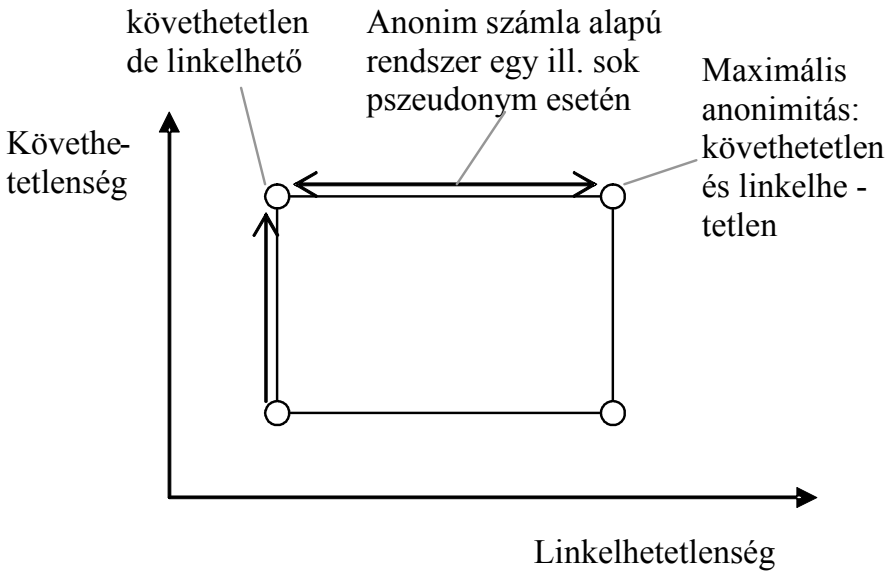
4.2. Anonimitás (Anonymity)

Az anonimitás a kézpénz természetes tulajdonsága, hiszen hagyományos esetében nem lehet összekapcsolni a vásárlást egy adott pénzdarabbal, tehát bizonyos fokú magánéleti védelmet, privacy-t nyújt a vásárlónak. Megjegyzendő, hogy szigorú értelemben véve a kézpénz nem feltétlenül teljesen anonim, például a vásárló látható a vásárlás során, ujjlenyomatot hagy a pénzen, ott van a pénzen az egyedi sorozatszám. Azonban gyakorlatban kivitelezhetetlen lenne ezeket az adatokat megfigyelni. Digitális pénz esetén más a helyzet, mert az informatikai eszközökkel végzett adatelemzés kivitelezhető, ha ez ellen nem használunk védelmi technológiákat. A digitális pénzben szerencsére megvan az anonimitás lehetősége, amit (főleg ideális digitális pénzrendszer esetében) szigorúan meg is követelünk.

A biztonság után tehát második legfontosabb tulajdonság a privacy védelme illetve az anonimitás. Ezeket a biztonsághoz hasonlóan szintén különböző kriptográfiai módszerekkel érik el a kutatók. A biztonságnál elmondottakhoz hasonlóan egyrészt lényeges, hogy mely problémákra lehet visszavezetni az alkalmazott protokoll feltörésének nehézségét, másrészt hogy a visszavezethetőség teljes egészében vagy csak részben bizonyított-e formális módszerekkel. Egy ideális rendszernél az anonimitásnak olyan számításelméleti probléma nehézségén kell nyugodnia, ami elfogadott és bizonyított.

Általában az anonimitásnak két fő szintjét különböztetik meg, melyeket az ideális rendszer is teljesít:

- Követhetetlenség (Untraceability): A digitális érmék és a felhasználók közötti kapcsolat követhetetlen.
- Linkelhetetlenség (Unlinkability): Ugyanazon (anonim) felhasználó által elköltött érmék között nem fedezhető fel semmilyen kapcsolat.



8. ábra: Az anonimitás szintjei

Az ideális rendszernél a tökéletes bűntény elkerülése végett az anonimitásnak jól szabályozott körülmények mellett visszavonhatónak kell kennie, azaz fair anonimitást kell biztosítania.

A PET (Privacy Enhancing Technologies) szaktekintélyek által használt és az informatikai biztonsági vizsgálatok módszertanát leíró Common Criteria-ban is szereplő négy tulajdonság (Anonymity, Pseudonimity, Unobservability, Unlinkability) illetve a tanulmányomban szereplő anonimitási és privacy tulajdonságok nem triviális kapcsolatban vannak egymással. A tudományos publikációk nem következetesen használják a különféle kifejezéseket, nagy a kavarodás. További információkkal kapcsolatban érdemes elolvasni a [PK01] publikációt, melyben Pfitzmann és Kohntopp megpróbálnak tájékozódni és rendet teremteni a szinonimák között. Az anonimitási tulajdonságnál lényeges, hogy kivel szembeni anonimitást vizsgálunk. A sémák célja, hogy a felhasználó tranzakciói különböző módon anonimak maradjanak a bankok, az üzletek és külső szemlélődők előtt.

A pszeudonimitási technikákkal a vásárlók személyének kiléte álcázható. A megfigyelhetetlenség (unobservabiliy) teljesül minden olyan entitásra, aki részt vesz egy tranzakcióban, azaz aki nem résztvevő fél, nem képes elolvasni a látott információkat. Emellett teljesül bizonyos információdarabokra is: egy protokoll során egyes adatok ugyanúgy láthatatlanok maradnak a megfelelő résztvevők előtt, mintha azok külső szemlélők volnának. Az összeköthetetlenség (unlinkability) az anonimitás egy magasabb szintje: ha például egy egyén kiléte álcázva van, akkor a különböző tranzakcióit nem képesek összefüggésbe hozni egymással a külső szemlélők vagy jogosulatlan felek (bankok). A kérdés azonban egyáltalán nem ilyen egyszerű. Már az is fogas kérdés, hogy definíció szerint mit takarhatnak ezek a tulajdonságok. Ennek az elektronikus fizetési rendszerekre tekintettel való további tisztázása meghaladja a publikáció kereteit [PK01].

4.3. A fair anonimitás tulajdonságai

A fair anonim rendszerekben háromféle nyomkövető eljárás terjedt el. Az ideális rendszerben értelemszerűen mind a háromféle rendelkezésre áll. A két alapvető követési módszer (a pénzkivét-követés és az érmekövetés) egy-két korai fair anonim rendszertől eltekintve mind rendelkezésre állnak, míg a harmadik típusú csak néhány rendszerben található meg jelenleg.

1. Tulajdonos-nyomkövetés (owner tracing): megállapítja egy érme tulajdonosát (például [BGK95], [SPC95])
2. Érme-nyomkövetés (coin tracing): azonosít egy banktól kivett pénzt (például [SPC95]).
3. Egy érme- és egy pénzkivétel-információ ismeretében eldönti, hogy azok összetartoznak-e.

A tulajdonos-nyomkövetés lehetővé teszi trustee-k számára, hogy megállapítsák egy érme tulajdonosát a fizetés lezajlása után. Ennek az elsődleges feladata az, hogy lehetővé tegye a „fizetés utáni” nyomkövetést a nagy monetáris rendszerekre vonatkozó törvényi szabályozás alapján. A tulajdonos-nyomkövetés azonban nem alkalmas sokféle bűntény megakadályozására, hiszen a megkülönböztetők a vásárláson alapulnak (például időpont, összeg, üzlet), ahelyett, hogy valamilyen közvetlenül a pénzérmére jellemző tulajdonság lenne. Az érmekövetés, hasonlóan a sorozatszám-követéséhez, „vásárlás előtti” követést tesz lehetővé. Az érmekövetéssel a trustee képes azonosítani egy érmét, amit kivettek a bankból, és képes ezt az érmét egy vásárláshoz kapcsolni (mert a megkülönböztető közvetlenül az érméhez kapcsolódik). Ennek az elsődleges feladata az, hogy nyomon kövesse a csalásokat és más bűncselekményeket a sorszám-követéshez hasonlóan. (Valójában ez sokkal hatékonyabb annál, mivel az átadhatóság általában nem lehetséges a

digitális pénzrendszereknél, így ugyanaz a központi bank intézi a pénzkivétet és a pénzbetétet is).

A trustee-nak a protokollokban való részvétele alapján három különböző megközelítés képzelhető el (3.12.1. fejezet). Az ideális digitális pénzrendszerben hatékonysági okokból megköveteljük, hogy a trustee entitások off-line-ok legyenek, a követési algoritmusoktól pedig, hogy hatékonyak legyenek.

4.4. Atomicitás (Atomicity)

A kutatók az atomicitás három szintjét különítik el [Tyg96a] [Tyg96b] [ST96] (3.17. fejezet). Egy ideális rendszernél a legjobbat, tehát Garantált Kézbesítés szintű atomicitást lehet elvárni, ami a gyakorlati vásárlások során nagyon megnyugtató mind a vásárló, mind az eladó számára, és nagymértékben segítheti a rendszer esetleges elterjedését.

4.5. Hatékonyság (Efficiency)

A hatékonyság vásárlói és kereskedői oldalról azt jelenti, hogy a rendszer használatához megfizethető eszközök szükségesek, és a protokoll fázisok (számlanyitás, pénzkivétel, fizetés, beváltás) rövid idő alatt lezajlanak. Például kedvező, ha a fizetéskori várakozási idő nem haladja meg a pár másodpercet, nem kell várni percekig. Szintén ide kapcsolódik, hogy kedvező, ha a felhasználó nem érzi korlátozva magát, például az elektronikus pénztárcája nem csak néhány darab érmét képes tárolni, hanem jó pár tucatot.

Banki oldalról a hatékonyság azt jelenti, hogy a rendszer működtetéséhez szükséges eszközök megfizethetőek a bank számára, a séma által támasztott tárolási és számítási kapacitás nem irreálisan nagy. A nyomkövetési műveletek is belátható időn belül eredményt szolgáltatnak.

Látható, hogy a hatékonyság teljesítésénél sok paraméter közötti egyensúlyt kell megtalálni. A hatékonyság növelése sokszor a biztonság rovására megy, mert sokszor vagy világosan láthatóan gyengébbé válik a rendszer, vagy csak kevésbé kielégítő módon bizonyítható a séma e tulajdonsága.

Az ideális rendszer is hatékony. Ezzel nemcsak az biztosított, hogy a tranzakciókhoz kevés várakozási idő szükséges, hanem elkerülhető a nagyobb számítási kapacitást igénylő eszközök használata. Kisebb számítási és tárolási kapacitású eszközök esetén a vásárlói és az eladói oldalon is kisebb befektetéssel tudnak beszállni a rendszerbe a potenciális felhasználók. A banki oldalon szintén kívánatos a hatékonyság, ezzel nemcsak banki

oldalon takaríthatók meg költségek, de könnyebb biztosítani a rendelkezésre állást, a megbízhatóságot, a terheléses támadások elleni védelmet.

4.6. Off-line

Hasznos tulajdonsága egy fizetőeszköznek, ha úgy mehetnek végbe fizetési tranzakciók, hogy közben nem szükséges a bankhoz is csatlakozni. Ez lehetővé teheti, hogy a vásárlások anélkül menjenek végbe, hogy mindegyik érmét on-line leellenőriznék, és mindegyik a kommunikációs hálózathoz lenne kötve. Az off-line tulajdonság a digitális pénz tranzakciókat sokkal hasonlatosabbá teszi a mai papírpénz működéséhez.

Az off-line/on-line használhatóság egy egyszerű eldönthetőségi tulajdonság, ami persze nagyban befolyásolja a biztonsági, anonimitási, hatékonysági és egyéb tulajdonságokat.

4.7. Oszthatóság (Divisibility)

Előnyös tulajdonság, ha a vásárló a birtokában lévő digitális pénzt be tudja osztani a saját igényei szerint (vagy valamilyen módon visszajárót tud kapni) (3.19. fejezet). A legtöbb mai rendszerben ez nem megoldott, egy adott digitális érme fix értékű. Az oszthatósági tulajdonsággal rendelkező rendszerek esetén csökkenthetők a pénzváltással vagy visszajáróval járó kommunikációs és számítási költségek. Általánosságban véve a rendszer használhatóbbá válik, ezért egy ideális digitális pénzrendszer rendelkezik ezzel a tulajdonsággal.

Az oszthatóságnál még fontos, hogy az ideális rendszerben erre olyan megoldás álljon rendelkezésre, ami nem csökkenti a biztonságot, a bizonyíthatóságot, ugyanakkor a hatékonysága is a lehető legjobb.

Az oszthatóság hathat az összeköthetetlenség tulajdonságára (3.19. fejezet). Több oszthatósági sémában az al-érmék (sub-coins, sub-coupons) linkelhetők egymással. Ez az ideális digitális pénzrendszerben nem megengedhető, sőt általánosabban megfogalmazva nem gyengülhet az anonimitás és annak bizonyíthatósága sem.

4.8. Átadhatóság, átruházhatóság (Transferability, Peer-to-Peer)

Digitális pénz tranzakció végbemehet vásárlók között is. Ez a tulajdonság is hasonlatosabbá teheti a rendszert a mai pénzhez. Lehetővé válik például, hogy az ebédlőben a munkatársam kisegítsen valamennyi összeggel, ha éppen nincs megfelelő mennyiségű pénz a kártyámon.

Az átadhatóságot is szeretnénk elvárni egy ideális rendszertől, mégpedig mindenképpen úgy, hogy a többi tulajdonságot ne befolyásolja hátrányosan (itt elsősorban a biztonságra, bizonyíthatóságra, anonimitásra, követhetetlenségre, hatékonyságra gondolunk).

4.9. Elvesztésállóság (loss tolerance)

Az elvesztésállóság egyelőre még nem elterjedt, de a teljesség kedvéért ezt is elvárjuk az ideális digitális pénzrendszertől, hiszen ritkán, de bárkivel előfordulhat, hogy elhagyja a pénzét. Mindezt úgy, hogy a 3.21. fejezetben leírt követelmények teljesüljenek.

4.10. Skálázhatóság (Scaleable)

Egy jó digitális pénzrendszernek skálázhatónak kell lennie. Ez annyit jelent, hogy a teljesítményének nem szabad észrevehetően degradálódni sem a rendszerben résztvevő (regisztrált) felhasználók számának növekedésével, sem pedig a végbemenő fizetési tranzakciók számának növekedésével. Ezt úgy igyekeznek elérni a rendszer tervezői, hogy olyan algoritmusokat alkalmaznak, amelyek számításelméletileg minél kevésbé függenek ezektől a számoktól (például nem $O(N^3)$, hanem csak $O(N)$). Ezen felül egyébként is mindig minél kisebb számítási és kommunikációs költségre törekednek a tranzakciós lépéseknél, hogy sem a központi hardver számítási teljesítmény (ez a bankoknál koncentráltan jelenik meg), sem a banki kommunikációs sávszélesség ne legyen akadályozó tényező. Ez a tulajdonság erős átfedésben van a hatékonyság követelményével.

4.11. Modularitás

Egy digitális pénz séma esetében az az ideális, ha független a konkrétan alkalmazott vak aláírási protokolltól, így az új kutatási eredmények (mint például a Liskov-féle Amortized e-Cash publikációban található ElGamal alapú vak-aláírás séma, DLA-tól függ) nehézség nélkül beilleszthetők a rendszerbe, és a séma publikálásakor még jelen levő egyes biztonsági kételyek később eloszlathatóak. Nemcsak a vak aláírásnál kell egy ideális rendszert modulárissá tenni, hanem más séma építőelemeknél is. Például bárhol használnak hash függvényeket, ott célszerű, ha mind az SHA, mind az md5 kivonatkészítő függvények használhatók. Mindezeket együttvéve modularitásnak nevezik, mert az egyes építőelemek modulként szerepelnek és kicserélhetőek ugyanolyan funkcionalitású modulokra. Vannak sémák, amelyeknél a tervezők szem előtt tartották ezt a tulajdonságot, az ideális digitális pénzrendszernél is megköveteljük.

4.12. Teljesen kidolgozott, sok-résztvevős protokollok

Fontos, hogy a rendszer minden aspektusból ki legyen dolgozva. Ebbe beletartozik az is, hogy minden olyan protokoll lépés, ahol sok résztvevő fél lehet jelen (például vak aláírás, nyomkövetés), teljesen világosan és részletesen definiálva legyen. Sok rendszerben csak megemlítik, hogy több ombudsman is részt vehet a protokollban, de később a konkrét elemzésben a szereplők felállásában csak egy ombudsman van jelen. Valószínűleg azért járnak el így, mert akár eggyel több résztvevő fél jelenléte is jelentős mértékben megbonyolítaná a rendszer átláthatóságát, bizonyíthatóságát.

Egy ideális digitális pénzrendszer esetén azonban ezek ellenére is ki kell dolgozni teljesen a sémát. Több módszer is rendelkezésre áll, mint például a csoport-aláírások (3.14. fejezet), vagy a határérték kriptográfiával kiterjesztett megoldások (3.15. fejezet).

Egy jó példa a [CMS96] publikáció, amelyben többek között részletesen kidolgozták, hogy hogyan lehet az anonimitás-visszavonási képességeket elosztani több trustee között. A megvalósítás a Shamir-féle titokcsere sémán és a Feldman-féle ellenőrizhető titokcsere sémán alapul.

5. Nyitott kérdések és problémák a digitális pénzrendszerekkel kapcsolatban

Ebben a fejezetben olyan nyitott kérdéseket szeretnék felvetni az elektronikus pénz sémákkal kapcsolatban, amelyeket eddig nem oldottak meg megnyugtató módon, nem vizsgáltak még elég behatóan, esetleg teljesen nyitva állnak. Szeretnék néhányat bemutatni, illetve olyan fontos tényekre is felhívom a figyelmet (például az anonim kommunikáció szükségessége), amelyeket eddig csak megemlítettem.

5.1. Anonimitás

5.1.1. Anonim kommunikáció

Noha általában csak megemlítik vagy kihangsúlyozzák a szükségességét az elektronikus pénz sémák publikációiban, nagyon fontos, hogy a résztvevő felek között anonim kommunikáció folyjon, hogy a fizetőrendszer valóban teljesen anonim lehessen. Enélkül a küldő és a fogadó fél helyét az adott hálózaton azonosítani lehet, fejlettebb forgalomanalízis technikákkal pedig a megszerzett információkat még tovább lehet finomítani.

A jelenlegi internet infrastruktúra nem támogatja beépített módon az anonimitást [Szé98] [Tót02]. Egy socket kapcsolat két résztvevőjét a legtöbb esetben azonosítja a forrás és a cél IP cím. Első látásra egy kapcsolat forrás és cél IP címének elrejtése egy külső támadó elől lehetetlen feladatnak látszik. Szerencsére a Chaum mix paradigma [Cha81] felhasználásával kriptográfiai keverő gépekből fölépíthető egy olyan speciális infrastruktúra, amely anonim kommunikációt tud biztosítani [SGR97] [Tót01] [Tót02].

Ezek után érthető is, hogy a sémák publikációi nem foglalkoznak részletesen ezzel, hiszen a sémától független, hogy azt milyen kommunikációs közeg felett alkalmazzák. Nem a séma feladata, hogy a közeget anonim kommunikációra alkalmassá tegye.

5.1.2. Visszavonható anonimitás

Szintén az anonimitás kérdéskörébe tartozik, hogy a visszavonható anonimitású rendszerek jó megoldások-e a bűncselekmények elleni védekezésre. A 3.16. fejezetben elmondottak alapján elképzelhető, hogy alkalmazásuk súlyosabb bűncselekmények megjelenését vonja maga után, mint amilyenek ellen kifejlesztették őket. Nem tudom megítélni, hogy a vészjelzéses vonal használata kielégítő megoldás-e. Elképzelhető, hogy más jellegű rendszerek szükségesek a sikeres védekezéshez [Tót03, 10. fejezet].

5.2. Biztonság

Mint ahogy az összehasonlításból is látható, minden rendszerben vagy található olyan tétel, amely nem teljesen bizonyított, vagy van olyan tétel, amely csak részben bizonyítottan vezethető vissza valamilyen kriptográfiai feltételezésre. Az sem ritka, hogy bizonyítható a nehéz feladatra való visszavezethetőség, azonban a feladatnak a nehézsége maga nem elfogadott, mert vagy teljesen egyedi komplexitási probléma, vagy pedig nem bizonyítható. Ez a biztonság és az anonimitás feltörhetetlenségére is igaz. Ez ügyben még sok a tennivaló, például még az igen kiforrott [FTY98] rendszerben is azt javasolják a kutatók, hogy általánosabb feltételezésekre kellene visszavezetni a rendszer bizonyítását.

Nehéz a védekezés sok különleges támadással szemben. Azt már említettem, hogy a bankrablásos támadásokat kevés rendszer tudja érzékelni, és a legtöbbjüknek veszély esetén on-line módba kell átkapcsolnia. A bankrablásos támadással már aktívan foglalkoztak a kutatók. Azonban vannak elhanyagoltabbnak tűnő kérdések. Előfordulhat például, hogy egy felhasználó dupla költése esetén a bolt a rendelkezésére álló információkat felhasználva további fizetéseket végez az érme segítségével, és ez a bűncselekmény nem derül ki. Érdekes kérdés lehet, hogy a jelenlegi protokollok ellen véghezvihető-e olyan támadás, ami több fél szimultán részvételekor a protokollok egymásra hatását használja ki. Például egy

időpillanatban több rosszhiszemű felhasználó végez pénzkivétet, és a protokollok pontos ismeretében és bizonyos paraméterek megfelelő manipulálásával képesek lehetnek-e arra, hogy egy érvényesnek minősülő érmét előállítsanak. Ezekre a kérdésekre további támadhatósági vizsgálatok és protokoll-elemzések adhatják meg a választ. Sajnos az ilyen sok-résztvevős támadások elemzése automatikus vizsgáló eszközökkel jóval nehezebben végezhető el, mint egy két-résztvevős protokollé.

5.2.1. Nyilvános kulcsú infrastruktúra

Az anonim kommunikációhoz hasonlóan nem tárgyalják részletesen az adott új sémák publikációi az alkalmazott nyilvános kulcsú kriptográfia vonzatait. A kulcsok és tanúsítványok hitelesítése egy megbízható PKI infrastruktúra segítségével valósítható meg biztonságosan. Így a rendszer biztonságának egy része (extrém esetben egésze) maga a PKI biztonságán nyugszik. Sajnos azonban a PKI infrastruktúrák is sokféle támadásnak lehetnek kitéve (például tanúsítvány visszavonása kapcsán operáló támadások, időbeli egybeeséseket és tulajdonságokat kihasználó támadások), melyek kiküszöbölése adott esetben igen nehéz lehet.

Egy megfelelően működő PKI felállítása bonyolult feladat. Nem csak egyszerűen a megbízott CA központok hierarchikus kapcsolódásáról van szó. Mindegyik központnak bizonyítania kell hogy megfelelő, biztonságos eljárásokat, menedzsment technológiákat használ. A biztonságuk legalább annyira az implementációs részleteken és a szervezési kérdéseken, mint magán az alkalmazott rejtjelezési technikákon alapul. Jelenleg még nem eldönthető, hogy egy világszerte vertikálisan integrált PKI hálózat megfelelően és biztonsággal működhet-e.

5.2.2. Heurisztikus tervezés

Jelenleg a sémákat ad-hoc módszerrel, heurisztikusan tervezik a kutatók, így mindig kockázatként merül fel az emberi tévedés lehetősége. Felmerül, hogy esetleg elkerülte a rendszer tervezőinek a figyelmét valami, és a séma biztonsága vagy anonimitása feltörhető.

Az irodalomban már nem egyszer előfordult, hogy tudományos cikkekben megjelent rendszerek biztonsági szempontból elégtelenek voltak. Ezek közül az alábbiakban hármat megemlítek, így a tanulságok jobban levonhatóak lesznek.

5.2.2.1. Három rendszer feltörése

Pfitzmann és Waidner [PW92] rámutatott Damgard (a Crypto '88 konferencián publikált) rendszerének [Dam90] számos biztonsági és hatékonysági gyengeségére, gyakorlatilag feltörték több szempontból is. Damgard rendszere [Cha89] típusú (on-line, fix accountok, feltétel nélküli követhetetlenség, összeköthetetlenség). A [Dam90] esetében egyrészt problémák vannak bizonyos definíciókkal. Ugyanis [Dam90] definíciója szerint a követhetetlenség azt jelenti, hogy a pénzkivét protokoll során shannoni értelemben semmilyen információ nem szivárog ki a bank által aláírt R számról, vagyis az érme számáról. Azaz, amikor az érmét beváltják, akkor a bank nem ismeri fel. Eddig ez igaz is, azonban a beváltás során nemcsak magát az R számot, hanem az aláírást is felmutatja a vevő. Ezért hozzá kell venni a definícióhoz, hogy a bank nemcsak hogy nem láthatja az aláírást a pénzkivét során, hanem nem is tudhat semmilyen információt róla. Ez is szükséges a követhetetlenséghez. Másfelől probléma van az általános rendszerrel: a legtöbb bizonyíthatóan biztonságos aláíró sémában az aláíró bemenete nemcsak a kulcs, vagyis a séma nem memóriamentes. A [Dam90] nem ilyen, mindaddig, amíg aláírásról aláírásra változik a bemenet, információ szivároghat ki az aláírásokon keresztül (ezt [PW92] két aláírás sémára is bebizonyítja). Általánosságban véve a memóriával rendelkező aláírás sémák alkalmatlanok vak aláírási sémák kialakítására fizetési rendszerekben. A követhetetlenség megjavítása olymódon lehetséges, mint minden más bizonyíthatóan biztonságos rendszerben: a pénzbeváltás során az aláírást nem mutatják meg. Ehelyett a vásárló zero-knowledge módon bizonyítja, hogy rendelkezik azzal. Az aláírás mellett a duplaköltés érzékelése miatt az érme sorszámát mindenképpen fel kell mutatni. Ebből következik az az általános tény, hogy az érme sorszámát a pénzkivét során mindenképpen „vakolni” kell.

A Eurocrypt '94 konferencián Amiano és Crescenzo bemutattak egy követhetetlennek mondott, NI-ZKP-on alapuló, előfeldolgozást használó protokollt, a rendszert néhány általános kriptográfiai feltételezés alapján bizonyíthatóan biztonságosnak mondták. Pfitzmann, Schunter és Waidner megmutatták [PSW95], hogy ez a protokoll nem biztosít semmiféle követhetetlenséget, és más további gyengesége is van.

Az Amiano-Crescenzo rendszerben egy gyenge követhetetlenség definíció szerepel, ami szerint a rendszer akkor követhetetlen, ha a bank akármennyi pénzkivét és beváltás megfigyelése után sem állapíthatja meg, hogy melyik melyikhez tartozik, azaz, hogy ki kinek fizetett. Látható, hogy nincs kereskedők általi követhetetlenség, mert a definíció csak pénzkivéteket és betéteket említ, tulajdonképpen csak a bank szemszögéből nézi a problémát. Ráadásul ez nem csak figyelmetlenség, hiszen a protokoll duplaköltés-

érzékelése pont azon a tulajdonságon alapszik, hogy az üzlet azonosítja a vásárlót. Ez nem elfogadható, mert a követhetetlenséget bankok és üzletek mindenféle koalíciója ellen biztosítani kell, az üzlettel szembeni követhetetlenség legalább annyira fontos, mint a bankkal szembeni.

Azonban nem ez a fő hiba a követhetetlenségben: Amiano és Crescenzo NI-ZKP-t előfeldolgozással kombinálja. A pénzbetét során a banknak ellenőriznie kell, hogy érvényes-e az NI-ZKP. Ez az ellenőrzés az eredetileg pénzt kivevő felhasználóval való előfeldolgozási fázison múlik. Mint ahogy az eladónak is, a banknak is tudnia kell, hogy mely stringet használja az ellenőrzés protokollban. Az előfeldolgozási fázisban tudja a felhasználó kilétét, akivel a stringet generálta. Vagyis a vásárló visszakövetődött. Ez egy általános probléma az előfeldolgozással kombinált NI-ZKP-val, amíg az előfeldolgozás két résztvevős protokoll: bármely hivatkozás azonosítja a résztvevő felet. Ezért a valódi követhetetlenséghez lehetetlennek látszik a primitív használata. Ha az előfeldolgozás a számlanyitása előtt anonim módon történik, akkor is linkelhető a vevő, csak egy bizonyos idő után.

A követhetetlenség sérül a dupla költés érzékelésnél is. A rendszerben amíg nem találják meg az elkövetőt, addig a bank nem is tudja bizonyítani, hogy az érme duplán lett elköltve. Általános szabály a követhetetlen protokollokra, hogy a rossz cselekedetre vonatkozó bizonyítékokat fel kell mutatni, mielőtt bármilyen további érzékeny információt fednének fel bárkiről. Szintén a dupla költő megtalálásával kapcsolatos probléma, hogy ha valaki kétszer kap ugyanolyan pénzt, akkor dupla költőnek bélyegződik meg, és nem tudja bizonyítani az ártatlanságát. Ez kiküszöbölhető, ha a pénz átadásnál véletlen kihívást és tranzakció-azonosítót használnak. Non-interaktív esetre időpecsét alkalmazása képzelhető el.

Pfitzmann, Schunter és Waidner [PSW95] feltörte a Crescenzo által a CIAC '94 konferencián bizonyíthatóan biztonságosnak bemutatott rendszert is. A [Cres94] rendszer extrém non-interaktivitást alkalmaz, azonban ennek sajnos megvannak a következményei. A rendszer teljesen non-interaktív, még a pénzkivét is egy üzenetből áll. El kell vetni az ilyen fokú non-interaktivitást. Az, hogy nincs követhetetlenség, abból látható, hogy minden érmét egy string azonosít, amit pénzkivétnél broadcast-olnak, és az érmével kapcsolatos tranzakcióban minden tisztán megjelenik. A rendszerrel szemben vannak egyéb kriptográfiai biztonsági aggályok is.

5.2.2.2. A feltörések tanulságai

A problémák elkerülése érdekében célszerű a következő szempontokat figyelembe venni a rendszerek tervezése során:

- a sémához mindig legyen lefektetve pontos trust modell;
- pontos specifikációkra van szükség;
- bizonyíthatósággal rendelkező protokollok csak úgy definiálhatók, hogy ellenőrző protokoll is van hozzájuk megadva.

Az egyik legfőbb probléma az, hogy sok mindenre nincs még megfelelő definíció, a meglévő definíciók hiányosak, nem teljesek. A másik pedig maga a tény, hogy a sémákat heurisztikus módon tervezik, és nem lehet kizárni az emberi hibázást. Az emberi tévedés kockázatát csökkenteni lehet, ha valamilyen módon szisztematikusabban tervezik a rendszereket, és minél több esetben használnak automatikus protokoll-ellenőrző logikákat. Az automatikus modell-ellenőrzés tudományának alkalmazására komoly törekvések irányulnak, de kielégítő eredmény csak a jövőben várható.

5.2.3. Szisztematikus vizsgálat, automatikus tételbizonyítás

Ha nagy körültekintéssel és odafigyeléssel végezzük a rendszer tervezését, betartjuk a más rendszerek feltöréséből levont tanulságokat, akkor is fennáll a hibázás lehetősége. A heurisztikus tervezésből fakadó hibák elkerülésében nagy segítséget nyújthat, ha a rendszer absztrakt modelljét formalizálják, majd ennek tulajdonságait gépi szabályelemzőkkel bizonyítják.

Sok publikációnak az a célja, hogy valamilyen szempont szerint teljesen formálisan és automatikusan kategorizáljon elektronikus fizetési sémákat, vagy ritkább esetben más célú kriptográfiai protokollokat (például elektronikus szavazási rendszerek). Sokszor valamilyen automatikus tételbizonyító, szabályelemző, modell-ellenőrző eszközt használnak ehhez (például FDR rendszer), néha valamilyen egyedi protokoll- vagy rendszer-modellező eszközt alkalmaznak [Tan96] [HTWC96] [PSS00] [SPS00].

Két fő feladat, hogy egyrészt leképezzük az elemezni kívánt sémákat az adott elemző környezetbe, formalizáljuk őket egy adott nyelven. Ezt nagyon körültekintően és pontosan kell megtenni, a feladat nagy részét ez jelenti, cserében viszont sokkal jobban beleláthatunk a sémák „lelki világába” egy adott aspektusból, hiszen szinte kivesézzük a protokollt.

A feladat másik nagy része, hogy az elemezni kívánt tulajdonságot formalizáljuk. Ha mindez megvan, le kell futtatni az elemzőt, s az eredmények értékelése következhet.

A módszernek több hátránya is van általában. Egyrészt egyszerre csak egy tulajdonságra lehet koncentrálni a vizsgálatnál, mert két különböző tulajdonság elemzéséhez teljesen más szemszögből kell analizálni a rendszereket. Hiába használjuk ugyanazt a bizonyítót (például FDR), teljesen más egy adott protokoll biztonságának vagy atomicitási tulajdonságainak vizsgálata. Másrészt a sémák összetettsége miatt a kutatók sokszor egyszerűsítésekhez, elhanyagolásokhoz folyamodnak, hogy formalizálni és elemezni tudjanak. Viszont nagyon az eszünkbe kell vésni, hogy mik ezek az egyszerűsítések, nehogy az elemzési eredmények végül értéktelennek bizonyuljanak, vagy félrevezetők legyenek.

Egy-egy ilyen módszer előnye pont az automatikusság, a formalizáltság: megpróbáljuk kiküszöbölni az emberi tévedésből adódó hibákat. Ha fény derül egy hibára az adott protokollban, akkor előfordulhat, hogy az elemzés egyben útmutatást is nyújt ahhoz, hogy azt milyen módon lehetne kijavítani. Sok esetben, amikor két rendszert elemeznek egyszerre, ez meg is történik, általában van egy állatorvosi ló szerepét betöltő és egy „jobb" rendszer is. A végeredmény megmutatja a hiányosságokat, és ezekre sokszor javítási javaslatokat is közölnek.

Az ideális digitális pénzrendszer szempontjából elvárható, hogy legalább a legfontosabb tulajdonságok (biztonság, anonimitás, atomicitás) különböző aspektusai formális módszerekkel bizonyítva legyenek. Természetesen a formalizálás során ne legyen a rendszer túlzottan leegyszerűsítve (például sok-résztvevős protokoll két-résztvevős protokollra).

6. Konklúzió

Véleményem szerint a számos bemutatott probléma ellenére a kriptográfiai protokollok és egyéb tudományterületek együttes alkalmazásával technikailag megoldható egy olyan pénz protokoll létrehozása, amely ideálisan teljesíti az elvárásokat. Igaz ugyan, hogy ehhez még sok kutatásra van szükség, de úgy látom, hogy dinamikusan fejlődnek a megjelenő technikák, és végeredményben konvergálnak egy ideális megoldáshoz.

A legnagyobb probléma talán az, hogy az egyes kritikus kérdések tekintetében külön-külön többnyire már születtek kielégítő megoldások, azonban ezeket az eredményeket szintetizálni, integrálni kellene egy olyan egyesített rendszerbe is, amely az összes problémát egyszerre képes legyőzni. Ez a gondolat bizonyos értelemben implicit módon néhány publikációban megjelenik: sok rendszert modulárisan terveznek meg, gondolva

arra, hogy egyes építőelemei kicserélhetők legyenek más megoldásokra, és a rendszer ne függjön konkrét technológiáktól (például az RSA-tól vagy a blind-Schnorr aláírás valamely változatától, amelyet a hatékonyság növelése miatt alkalmaznak, miközben még elegendő biztonságot érnek el, tehát vállalják, hogy áldoznak a biztonságosság oltárán a hatékonyság kedvéért, stb.).

A hatékonyság terén még hosszú út áll előttünk. Sok szerző szerint a sikertelenség egyik legfőbb oka, hogy a digitális pénz paradigmán alapuló protokollok még csak korlátozottan alkalmasak a smart card-ok által jelentett erőforrásszegény környezetben való futtatásra. A hatékonysági problémák különösen a kis értékű fizetések esetén szembeötlők, ahol a tranzakció értékéhez képest aránytalanul nagyobb értéket képviselnek.

A mikrofizetési rendszerek technikai trükkökkel és az anonimitás vagy a biztonság nagyon körültekintő enyhítésével együttesen küszöbölik ki a gondot. Véleményem szerint semmilyen körülmények között, még mikrofizetési rendszerek esetében sem szabad a biztonság rovására csökkenteni a költségeket, mert egy ilyen döntés később nagyon megbosszulhatja magát. Olyan kriptográfiai, matematikai, technikai trükkökkel szabad csak növelni a hatékonyságot, amelyek sem az anonimitást, sem a biztonságot nem csökkentik. Például az általam vizsgált publikációkban nem találkoztam az elliptikus-görbe rejtjelezés használatával, pedig ez kifejezetten smart card környezetben lehet előnyös: alkalmazásával ugyanolyan biztonságot kisebb számítási teljesítménnyel is el lehet érni.

A hatékonysági vonalon egyelőre azt sikerült elérni, hogy a tranzakciós várakozási idők elfogadható időn belül vannak (fél másodperc). A sémák oldaláról szemlélődve nem sok bizakodásra adhat okot [FTY98], amelyben a kutatók úgy vélik, hogy a rendszer hatékonyságán már nem lehet számottevően javítani. Szerencsére a technológia hihetetlen iramú fejlődése előbb-utóbb mindenképpen segíteni fog, de talán segíthetnek olyan technológiai vívmányok is, mint az elliptikus-görbe rejtjelezések.

Az [FTY98]-ra visszatérve, a hatékonyság csak egy a fontos követelmények közül, mert a kutatók a legnagyobb problémának azt látják, hogy a biztonságot sokkal szigorúbb feltételek mellett is bizonyítani lehessen. Iránymutatást azért adnak: szerintük egy lehetőség egy olyan új homomorf tulajdonsággal rendelkező rejtjelezési séma, amelynek biztonsága a factoring feladat nehézségével egyenlő (egy ilyet dolgozott ki Okamoto-Uchiyama). Olyan „vakolási” protokollok is hiányoznak, amelyek korlátozó tulajdonsága bizonyítható. Tehát kriptográfiai és matematikai téren is még mindig sok munka van hátra.

A digitális pénznek az előnyei alapján simán lenne esélye olyan népszerűvé válnia, mint más elektronikus fizetési módszerek vagy éppenséggel a papírpénz. A digitális

pénzrendszerek általános elterjesztésére irányuló törekvések eddig azonban nem jártak sikerrel. A sikertelenségnek sok oka van, ezekkel külön irodalom foglalkozik. Az biztos, hogy jelenleg még nem létezik olyan séma, ami minden elvárást ideálisan teljesít. Számos technológia (mint például az irányítható anonimitás) még kutatás alatt áll.

Optimista vagyok és bizakodó, és azt vallom, hogy előbb-utóbb biztosan elérkezik az a pillanat, amikor a különféle részterületeken elért eredményeket összefogják, és minden eddigi tapasztalatot és tanulságot figyelembe véve elkészül egy összetett rendszer a részletes bizonyításokkal, formális modellekkel és bizonyításokkal együtt.

E tanulmány megszívlelendő mottója mellé zárásképpen a következő idézett ajánlom az olvasó figyelmébe [BZ03]: „*Veszélyes játékot játszanak azok a tervezők, akik »pont elégségesen erős« algoritmusokat készítenek, és a sebesség érdekében engednek a robosztusságból. Példa erre a mobiltelefonok A5 rejtjelező algoritmusának feltörése."*

Rövidítésjegyzék

CA (Certification Authority, Tanúsítvány-kiállító hatóság)
Olyan hitelesítés-szolgáltató, amely digitális tanúsítványokat állít ki személyek részére. A hitelesítés-szolgáltatók maguk is rendelkeznek tanúsítvánnyal, amelyet magasabb rangú CA-k bocsátanak ki számukra.

DHA (Diffie-Hellman Assumption)
Egy sejtés, amely szerint a Diffie és Hellman által megfogalmazott probléma megoldhatatlan. A DHA nehézsége a DLA-n alapszik.

DLA (Discrete Logarithm Assumption, diszkrét logaritmus feltételezés)
Egy sejtés, amely a diszkrét logaritmusokkal kapcsolatban egy megoldhatatlan feladatot fogalmaz meg.

DoS (Denial of Service)
Olyan informatikai támadás, ahol a cél egy szolgáltatás működésének megakadályozása a rendszer túlterhelésével.

DSA (Digital Signature Algorithm)
A DSS szabvány által definiált digitális aláírás séma.

FOLC (Fair Off-Line Cash)
Olyan OLC, amelyben az anonimitás visszavonható.

IP (Internet Protocol)
Az internet hálózati rétegének világszabvány szerinti protokollja.

IP-cím (Internet Protocol-cím)
Pontokkal osztott adott formátumú számsor, amely azonosítja az internetre csatlakoztatott számítógépet.

MI-DSS (Magic Ink DSS: DSS alapú mágikus tintás aláírás)
Olyan mágikus tintás aláírás, amely a megvalósításhoz a DSS szabványban definiált DSA sémát használja.

OLC (Off-Line Cash)
Off-line tulajdonságokkal rendelkező digitális pénz séma.

PDA (Personal Digital Assistant)
Általában tenyérnyi (palm) méretű digitális személyi asszisztens, kéziszámítógép. A smart card-nál nagyobb számítási teljesítménnyel rendelkezik, input perifériák is találhatók rajta (kis méretű klaviatúra, mikrofon, érintőképernyő), ezért különösen alkalmas lehet a digitális pénztárca funkciók betöltésére. Hátránya, hogy kevésbé tekinthető manipulálás-védett eszköznek, mint a smart card.

PIN (Personal Identification Number)
Alfanumerikus karakterekből álló kód, amely a felhasználó titkát képezi. Általában engedélyezés kapcsán használják, például ezzel védik a felhasználó PDA-ját az illetéktelen hozzáférések ellen.

PKI (Public Key Infrastructure, Nyilvános kulcsú infrastruktúra)
Azon technológiák, eljárások és intézmények összessége, amelyek segítségével a nyilvános kulcsok kezelése, tárolása és felhasználása megbízható módon véghezvihető. A PKI részei többek között a CA-k (tanúsítvány kiállító hatóságok) és az RA-k (kulcskibocsátó hatóságok).

QRA (Quadratic Residue Assumption)
Egy sejtés, amely a kvadratikus maradékokkal kapcsolatban egy megoldhatatlan feladatot fogalmaz meg.

RSA (Rivest, Shamir, Adlemann)
A feltalálóiról elnevezett szabványos nyilvános kulcsú rejtjelező algoritmus.

TRD (Tamper Resistent Device, manipulálás-védett eszköz)
Olyan elektronikus eszköz, amelynek a tartalmát és a működését nem tudja a felhasználó befolyásolni, megváltoztatni. A smart card-ot sokszor TRD-nek tekintik.

TTP (Trusted Third Party, megbízható harmadik fél, trustee, ombudsman)
Titok letétbe-helyezési ágens, amely az elektronikus pénzrendszerben olyan információkhoz jut, amelyek szükségesek a felhasználó de-anonimizálásához.

Hivatkozások jegyzéke

Ant90
H. van Antwerpen: *Off-line Electronic Cash,* Master's thesis, Eindhoven University of Technology, Department of Mathematics and Computer Science, 1990.

Bra93
S. Brands: Untraceable Off-line Cash in Wallets with Observers (Extended abstract), *Proceedings of Crypto '93,* LNCS Vol. 773, p 302–318, 1994.

Bra94
S. Brands: Off-Line Cash Transfer by Smart Cards, Centrum voor Wiskunde en Informatica, Report CS-R9455, 1994 September. Also in: *Proceedings of the First Smart Card Research and Advanced Application Conference,* France, p. 101–117, 1994 October.

Bra95a
S. Brands: Electronic Cash on the Internet, *Proceedings of the Internet Society Symposium on Network and Distributed System Security,* San Diego, California, 1995 February.

Bra95b
S. Brands: Off-Line Electronic Cash Based on Secret-Key Certificates, *Proceedings of the Second International Symposium of Latin American Theoretical Informatics (LATIN '95),* Chili, April 3–7, 1995. Also in: Centrum voor Wiskunde en Informatica, Report CS-R9506, 1995.

BC90
J. Bos, D. Chaum: *SmartCash: A Practical Electronic Payment System,* Technical Report CS-R9035, Centrum voor Wiskunde en Informatica, Amsterdam, 1990 August.

BGK95
E. Brickell, P. Gemmell, D. Kravitz: Trustee-based Tracing Extensions to Anonymous Cash and the Making of Anonymous Change, *Proceedings of 6th Annual ACM-SIAM Symposium on Distributed Algorithms (SODA),* p. 457–466, ACM Press, 1995 January.

BZ03
M. Bond, P. Zielin'ski: *Decimalisation table attacks for PIN cracking,* Technical Report Number 560, ISSN 1476-2986, UCAM-CL-TR-560, University of Cambridge, 2003 February.

Cam97
J. Camenisch: Efficient and Generalized Group Signatures, *Proceedings of Eurocrypt '97,* Konstanz, Germany, 1997 May, LNCS Vol. 1233, p. 465–479, 1997.

Cha81
D. Chaum: Untraceable Electronic Mail, Return Addressess, and Digital Pseudonyms, *Communications of the ACM* Vol. 24, No. 2, p. 84–88, 1981.

Cha83
D. Chaum: Blind Signatures for Untraceable Payments, *Proceedings of Crypto '82,* p. 199–203, Plenum Press, New York and London, 1983.

Cha89
D. Chaum: Privacy Protected Payments Unconditional Payer and/or Payee Untraceability, *Proceedings of Smart Card 2000,* North-Holland, Amsterdam, p. 69–93, 1989.

Cha90
D. Chaum: Online Cash Checks, *Proceedings of Eurocrypt '89,* LNCS Vol. 434, p. 288–293, 1990.

Cha92
D. Chaum: Achieving Electronic Privacy, *Scientific American,* August 1992, p. 96–101.

Cox94
B. T. H. Cox: *Maintaining Privacy in Electronic Transactions,* Master's thesis, Carnegie Mellon University, Information Networking Institute, Pittsburgh, Pennsylvania, 1994 August.

CFN90
D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash, *Proceedings of Crypto '88,* LNCS Vol. 403, p. 319–327, 1990.

CFT98
A. Chan, Y. Frankel, Y. Tsiounis: Easy come — easy go divisible cash, *Proceedings of Eurocrypt '98,* Helsinki, Finland, LNCS Vol. 1403, p. 561–575, 1998.

CH91
D. Chaum, E. van Heijst: Group Signatures, *Proceedings of Eurocrypt '91,* LNCS Vol. 547, p 257–265, 1992.

CMS96
J. Camenisch, U. Maurer, M. Stadler: Digital Payment Systems with Passive Anonimity-Revoking Trustees, *Proceedings of ESORICS 96,* LNCS Vol. 1146, p. 33–43, 1996.

CP92
D. Chaum, T. Pedersen: Wallet Database with Observers, *Proceedings of Crypto '92,* LNCS Vol. 740, p. 89–105, 1992.

CP93a
D. Chaum, T. P. Pedersen: Transferred Cash Grows in Size, *Proceedings of Eurocrypt '92,* LNCS Vol. 658, p. 390–407, 1993.

CP93b
R. J. F. Cramer, T. P. Pedersen: Improved Privacy in Wallets with Observers, *Proceedings of Eurocrypt '93,* LNCS Vol. 765, p. 329–343, 1994.

CPS96
J. Camenisch, J-M. Pivateau, M. Stadler: An Efficient Fair Payment System, *Proceedings of 3rd ACM Conference on Computer and Communication Security,* New Delhi, p. 88–94, 1996 March.

CPV99
J. Claessens , B. Preneel , and J. Vandewalle: Anonymity Controlled Electronic Payment Systems, *Proceedings of the 20th Symposium on Information Theory in the Benelux,* p. 109–116, 1999.

CS97
J. Camenisch, M. Stadler: Efficient Group Signature Schemes for Large Groups (Extended Abstract), *Proceedings of Crypto '97,* Santa Barbara, California, August, LNCS Vol. 1294, p. 410–424, 1997.

Dam90
I. B. Damgard: Payment Systems and Credential Mechanisms with Provable Security Against Abuse by Individuals, *Proceedings of Crypto '88,* LNCS Vol. 403, p. 328–335, 1990.

DFTY97
G.I. Davida, Y. Frankel, Y. Tsiounis, M. Yung: Anonymity Control in E-Cash Systems, *Proceedings of Financial Cryptography '97,* Anguilla, British West Indies, p. 1–16, 1997 February.

EO95
T. Eng, T. Okamoto: Single-Term Divisible Electronic Coins, *Proceedings of Eurocrypt '94,* p. 306–319, 1995.

Fer94
N. Ferguson: Single Term Off-Line Coins, *Proceedings of Eurocrypt '93,* LNCS Vol. 765, p. 318–328, 1994.

Fer95
N. Ferguson: Extension of Single-Term Coins, *Proceedings of Crypto '93,* p. 292–301, 1994.

FP186
National Institute of Standards and Technology: *Digital Signature Standard (DSS),* Federal Information Processing Standards Publication 186-2 (FIPS PUB 186-2), 2000 January 27.

FTY96
Y. Frankel, Y. Tsiounis, M. Yung: "Indirect Discourse Proofs": Achieving Efficient Fair Off-Line E-Cash, *Proceedings of Asiacrypt '96,* 1996 November, South Korea, LNCS Vol. 1163, p. 286–300, 1996.

FTY98
Y. Frankel, Y. Tsiounis, M. Yung: Fair Off-Line e-Cash made easy, *Proceedings of Asiacrypt '98,* Beijing, China, 1998 October, p. 257–270, 1998.

FY92
M. Franklin, M. Yung: Towards Provably Secure Efficient Electronic Cash (extended abstract), Columbia University, Department of Computer Scinece, TR CUCS-018-92, 1992 April 24.

FY93
M. Franklin, M. Yung: Secure and Efficient Off-Line Digital Money, *Proceedings of ICALP 1993,* Lund, Sweden, 1993 July, LNCS Vol. 700, . 265–276, 1993.

FY94a
M. Franklin, M. Yung: Blind weak signatures and its application: Putting non-cryptographic computation to work, *Proceedings of Eurocrypt '94,* p. 71–83, 1994.

FY94b
M. Franklin, M. Yung: The Blinding of Weak Signatures (extended abstract), *Proceedings of Eurocrypt '94,* p. 67–76, 1994.

HTWC96
N. Heintze, J.D. Tygar, J. Wing, H. Chi Wong: Model Checking Electronic Commerce Protocols, *Proceedings of the 2nd USENIX Workshop on Electronic Commerce,* p. 147–164, Oakland, California, 1996 November.

Jak95
M. Jakobsson: Ripping Coins for a Fair Exchange, *Proceedings of Eurocrypt '95,* LNCS Vol. 921, p. 220–230, 1995.

Jak97
M. Jakobsson: *Privacy vs. Authenticity,* PhD Thesis, University of California, San Diego, 1997.

JY96
M. Jakobsson, M. Yung: Revokable and Versatile Electronic Money (Extended Abstract), *Proceedings of 3rd ACM Conference on Computer and Communication Security,* p. 76–87, New Delhi, 1996 March.

JY97
M. Jakobsson, M. Yung: Distributed "Magic Ink" Signatures, *Proceedings of Eurocrypt '97,* LNCS Vol. 1233, p. 450–464, 1997.

JM99
M. Jakobsson, J Müller: Improved Magic Ink Signatures Using Hints, *Proceedings of Financial Cryptography '99,* LNCS Vol. 1648, p. 253–267, 1999.

LR98
A. Lysyanskaya, Z. Ramzan: Group Blind Digital Signatures: A Scalable Solution to Electronic Cash, *Proceedings of Financial Cryptography '98,* LNCS Vol. 1465, p. 184–197, 1998.

Oka92
T. Okamoto: Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes, *Proceedings of Crypto '92,* LNCS Vol. 740, p. 31–53, 1992.

Oka95
T. Okamoto: An Efficient Divisible Electronic Cash Scheme, *Proceedings of Crypto '95,* LNCS Vol. 963, p. 438–452, 1995.

OO92
T. Okamoto, K. Ohta: Universal Electronic Cash, *Proceedings of Crypto '91,* LNCS Vol. 576, p. 324–337, 1992.

Pet97
H. Petersen: How to convert any digital signature scheme into a group signature scheme, *Proceedings of Security Protocols Workshop '97,* Paris, LNCS Vol. 1361, p. 177–190, 1997.

PK01
A. Pfitzmann, M. Kohntopp: Anonymity, unobservability, and pseudonymity — a proposal for terminology, *Proceedings of International Workshop on Design Issues in Anonymity and Unobservability,* July 2000, LNCS Vol. 2009, p. 141–160, 2001.

PSS00
A. Popovici, H. Schuldt, H.-J. Schek: Generation and Verification of Heterogeneous Purchase Processes, *Proceedings of the 1st International Workshop on Technologies for E-Services (TES'2000),* Cairo, Egypt, 2000 September.

PSW95
B. Pfitzmann, M. Schunter, M. Waidner: How to Break Another "Provably Secure" Payment System, *Proceedings of Eurocrypt '95,* LNCS Vol. 921, p. 121–132, 1995.

PW92
B. Pfitzmann, M. Waidner: How to Break and Repair a "Provably Secure" Payment System (Extended Abstract), *Proceedings of Crypto '91,* LNCS Vol. 576, p. 338–350, 1991.

PW95
B. Pfitzmann, M. Waidner: Strong Loss Tolerance for Untraceable Electronic Coin Systems, *Hildesheimer Informatik-Berichte* 1995, Vol. 15, ISSN 0941-3014, Institut für Informatik, Universität Hildesheim, 1995 June.

PW97
B. Pfitzmann, M. Waidner: Strong Loss Tolerance of Electronic Coin Systems, *ACM Trasactions on Computer Systems,* Vol. 15, No. 2, p. 194–213, 1997 May.

Sch91
C. P. Schnorr: Efficient Signature Generation for Smart Cards, *Proceedings of Crypto '89,* LNCS Vol. 435, p. 239–252, 1989. Later in *Journal of Cryptology,* Vol. 4, No. 3, p. 161–174, 1991.

Sch96
B. Schneier: *Applied Cryptography,* 2nd ed., p. 139–147, 1996.

SGR97
P. F. Syverson, D. M. Goldschlag and M. G. Reed: Anonymous Connections and Onion Routing. *Proceedings of the Symposium on Security and Privacy,* Oakland, CA, p. 44–54, 1997 May.

SN92
S. von Solms, D. Naccache: On Blind Signatures and Perfect Crimes, *Computers and Security,* Vol. 11, No. 6, p. 581–583, 1992.

SP99
H. Schuldt, A. Popovici: Transactions and Electronic Commerce, *Proceedings of the 8th International FMLDO Workshop: Transactions and Database Dynamics (TDD'99),* Schloss Dagstuhl, Germany, 1999 September, LNCS Vol. 1773, p. 225–230, 1999.

SPC95
M. Stadler, J-M. Pivateau, J. Camenisch: Fair Blind Signatures, *Proceedings of Eurocrypt '95,* LNCS Vol. 921, p. 209–219, 1995.

SPS99a
H. Schuldt, A. Popovici, H-J. Schek: Execution Guarantees in Electronic Commerce Payments, *Proceedings of the 8th International FMLDO Workshop: Transactions and Database Dynamics (TDD'99),* Schloss Dagstuhl, Germany, 1999 September, LNCS Vol. 1773, p. 193–202, 1999.

SPS99b
H. Schuldt, A. Popovici, H.-J. Schek: Give me all I pay for — Execution Guarantees in Electronic Commerce Payment Processes, *Proceedings of the Informatik '99 Workshop,* Paderborn, Germany, 1999 October 6.

SPS00
H. Schuldt, A. Popovici, H.-J. Schek: Automatic Generation of Reliable E-Commerce Payment Processes, *Proceedings of the 1st International Conference on Web Information Systems Engineering (WISE'2000),* p. 434–441, Hong Kong, China, IEEE Computer Society, 2000 June.

ST96
J. Su, J. D. Tygar: Building Blocks for Atomicity in Electronic Commerce, *Proceedings of the 6th USENIX UNIX Security Symposium,* San Jose, California, 1996 July.

Szé98
Székely Iván: A jó, a rossz, meg az anonim remailer, *Magyar Távközlés,* Vol. IX., No. 5., Budapest, 1998.

Szé00
Székely Iván: PET technológiák: a személyes adatok védelmének korszerű eszközei.
In: *Létezik-e adatvédelem adatbiztonság nélkül?*
Infoszféra Kft., Budapest 2000.

Tan96
L. Tang: Verifiable Transaction Atomicity for Electronic Payment Protocols, *Proceedings of the 16th International Conference on Distributed Computing Systems,* p. 261–269, IEEE Computer Society, 1996 May.

Tót01
Tóth, Csaba: *Privát web böngészés onion routing technológia segítségével,* BME VIK Híradástechnika Tanszék, Diplomaterv, Budapest, 2001. május.

Tót02
Tóth, Csaba: Anonim kommunikáció és a proxy szerverek, BME GTK Információ- és Tudásmenedzsment Tanszék, *ALMA MATER: Sokszínű e-világ,* p. 145–164, Budapest, 2002. február.

Tót03
Tóth, Csaba: *Digitális pénzrendszerek anonimitási és biztonsági vizsgálata,* BME GTK Információ- és Tudásmenedzsment Tanszék, Diplomaterv, Budapest, 2003. június.

Tyg96a
J. D. Tygar: *Atomicity in Electronic Commerce,* research report CMU-CS-96-112, Carnegie Mellon University, Computer Science Department, Pittsburgh, 1996 January.

Tyg96b
J. D. Tygar: Atomicity in Electronic Commerce, *Proceedings of the 15th Annual ACM Symposium on Principles of Distributed Computing,* p. 8–26, Philadelphia, Pennsylvania, 1996 May.

WP90
M. Waidner, B. Pfitzmann: Loss-Tolerance for Electronic Wallets, *Proceedings 20th International Symposium on Fault-Tolerant Computing (FTCS 20),* p. 140–147, Newcastle upon Tyne, UK, 1990.