Budapesti Műszaki és Gazdaságtudományi Egyetem
Hálózati Rendszerek és Szolgáltatások Tanszék

Adatpiacokban felmerülő kriptográfiai problémák

Ph.D. Tézisfüzet

Horváth Máté

Konzulens: Buttyán Levente, Ph.D.

Budapest
2020

Köszönetnyilvánítás

Ezúton szeretném kifejezni köszönetemet a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal,[1,2] a MELLODDY projekt,[3] és a CELSA Kutatási Alap támogatásáért valamint a Csibi Sándor ösztöndíjért.

Rövidítések jegyzéke

2PC	secure two-party computation
ABE	attribute-based encryption
CKA2	adaptive chosen keyword attack
CP-ABE	ciphertext-policy attribute-based encryption
CPFE	controlled private function evaluation
DDH	döntési Diffie–Hellman feltevés
EU-CMA	existential unforgeability under chosen message attack
FE	functional encryption
IND-CKA2	indistinguishability under adaptive chosen keyword attack
IND-CPA	indistinguishability under chosen plaintext attack
IoT	internet of things
MAC	message authentication code
OT	oblivious transfer
PFE	private function evaluation
rCPFE	relaxed controlled private function evaluation
RL	revocation list
SSE	searchable symmetric-key encryption
SXDH	symmetric external Diffie–Hellman assumption
UC	universal circuit

[1]Az itt bemutatott kutatás a Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal – NKFIH, 116675 (K) támogatásával készült.

[2]A kutatást az „IoT rendszerek biztonságát növelő technológiák” projekt(2018-1.2.1-NKP-2018-00004)című projekt támogatta a Nemzeti Kutatási és Innovációs Alapból biztosított támogatással, a „Nemzeti Kiválósági Program:2018-1.2.1-NKP” pályázati program finanszírozásában valósult meg (2018-1.2.1-NKP-2018-00004).

[3]A projektet támogatta az „Innovative Medicines Initiative 2” nevű közös vállalkozás (N° 831472). A közös vállalkozást az Európai Unió Horizon 2020 nevű kutatási és innovációs programja és az EFPIA támogatja.

1. Bevezetés

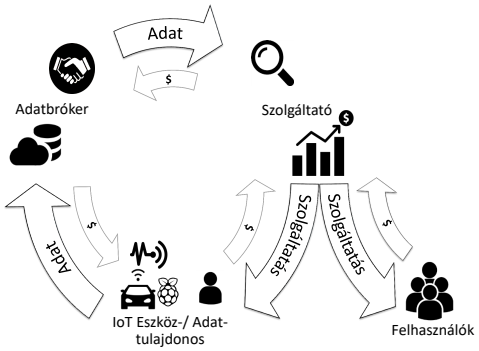
Az elmúlt évtizedek megmutatták, hogy mindennapjainkban egy paradigmaváltáson megyünk keresztül: a fizikai dolgokat digitális megfelelőik váltják fel. Az elmúlt évek tapasztalata, hogy a változás üteme egyre gyorsul. Az ezzel járó egyik legnagyobb kihívás, hogy a virtuális világban számos olyan dolgot kell garantálnunk, melyek a fizikai világban természetes módon adottak voltak. Kitűnő példa erre a bizalom. Ha Aliz besétál egy üzletbe, ahol egy órát tölt el a kedvenc ruhája kiválasztásával, majd készpénzzel fizet, akkor boldogan hazafelé tartva aligha kell attól tartania, hogy vásárlása bárkinek lehetőséget adhatott volna az elmúlt havi fizetésének megszerzésére, ízlésének vagy ruhaméretének megfigyelésére, esetleg lakcímének kiderítésére. Ezek a lopás és kémkedés számba menő dolgok nemcsak elszántságot, hanem jelentős erőfeszítést is követelnek a fizikai világban, ezért általában megbízhatunk abban, hogy nem követik el ezeket ellenünk. Azonban, ugyanezek a dolgok a virtuális világban (pl. egy webáruházban) sokkal „veszélyesebbek", hiszen egy teljes iparág épült az Alizhoz hasonló vásárlók utáni kémkedésre és a különössen értékesnek bizonyuló adataik gyűjtésére [EN16]. Ennek következménye, hogy a bizalom nem lehet többé magától értetődő.

Boaz Barak szellemes meghatározása szerint a „kriptográfia célja a bizalom helyettesítése matematikával" [Bar16]. Ez a megfigyelés rávilágít a kriptográfia növekvő szerepére a mindennapi életünkben. A virtuális lehetőségek bővülésével a létező kriptográfiai módszerek újabb és újabb alkalmazásokra találnak, de számos esetben van szükség új módszerek fejlesztésére is, ami folyamatos kihívást jelent a kriptográfiában.

Disszertációmban a kialakulóban lévő adatpiacok és a kriptográfia kapcsolatát vizsgálom. Napjainkban az adatok növekvő jelentősége megkérdőjelezhetetlen. Egy EU jelentés szerint [CMM+20] „az adatgazdaság összértéke, ami az adatpiac teljes hatását méri a gazdaság egészére nézve, 2019-ben átlépte a 400 milliárd €-t az EU 27 tagállamát és az Egyesült Királyságot tekintve, ami 7,6%-os növekedés az előző évhez képest." A nagy számok ellenére, napjainkban az adatgazdaság szereplői többnyire nagyvállalatok, míg a végfelhasználók leginkább az adatgyűjtés fő forrásai ahelyett, hogy valódi szerepük lenne a piacon. Az aktuális technológiai trendek, mint az okos eszközök és az ún. dolgok internete (vagy internet of things (IoT)), változtathatnak ezen a helyzeten, hiszen gyorsan növekvő mennyiségű adatot generálnak, ami mind felhasználásra vár. Ennek legfőbb korlátja, hogy a legtöbb esetben az összegyűjtött adatok csak a felhasználó és az eszköz gyártója számára érhetők el. Egy lehetséges módja a információban rejlő lehetőségek jobb kihasználásának ha egy ökoszisztémát építünk az adatok köré. Pontosan ez az adatpiac alapötlete is, melynek koncepcióját az 1. ábra szemlélteti. Itt az adatbróker nyers adatot vásárol az adatokat gyűjtő eszközök tulajdonosaitól és az így gyűjtött adatokat árulja (esetleg saját számítási kapacitásával együtt) olyan szolgáltatóknak, akik adatok feldolgozásán alapuló szolgáltatásokat (pl. előrejelzéseket) árulnak felhasználóiknak.

Az adatpiacok számos megközelítése került át a gyakorlatba a közelmúltban [Oce, Dat17, IOT, Dat]. Munkám során a lehetséges megvalósítások által felvetett biztonsági kérdéseket vizsgáltam.

Első lépésként egy általános rendszermodellel írtam le az adatpiacok lehetséges mű-



1. ábra. Centralizált adatpiac sematikus modellje.

ködését és erre a modellre alapozva elemeztem a résztvevők lehetséges biztonsági igényei által meghatározott piacokat. Ehhez azonosítottam azokat a lehetséges szcenáriókat, melyeket a szereplők lehetséges céljai, egymással szembeni bizalma és az ebből következő biztonsági követelmények meghatároznak. Ezeket a szcenáriókat aztán a kriptográfia különböző területeivel kapcsoltam össze, ami egyrészt segíti a felmerülő biztonsági problémákra adható válaszok keresését, másrészt nyitott kriptográfiai problémákra világít rá. Az azonosított kutatási irányok közül ezután hárommal részletesen is foglalkoztam.

A vizsgált problémákban közös, hogy hatékony megoldásukhoz egymásnak ellentmondó igényeknek kellene megfelelni, amik szükségszerű korlátokat jelentenek bármilyen megoldás számára. Ezek között az egymásnak feszülő korlátok között kerestem minden esetben a kompromisszumot, ami közelebb vihet egy a korábbiaknál jobb megoldáshoz.

Az első problémát a privát függvény kiértékelés (PFE) protokollok résztvevői közti érdekellentét jelentette. Egyikük célja a közös számításban felhasznált adat (a függvény bemenete) míg másikuké a kiértékelt függvény elrejtése a másik résztvevő elől. Feltéve, hogy a függvényt szolgáltató fél hozzáfér a számítás kimenetéhez, a legtöbb amit elvárhatunk egy PFE protokolltól az az, hogy ne fedjen fel több információt a bemenetről, mint amit a kimenet már önmagában felfed. Még ha a teljes bemenet nem is kompromittálódik ilyen módon (a kimenet hossza tipikusan rövidebb a bemenet hosszánál), a protokoll futtatásának kezdetén a bemenet tulajdonosa aligha tudhatja, hogy mit fog felfedni az adatáról. Ebből a problémából kiindulva kezdeményeztem a részinformáció szivárgásának vizsgálatát ebben a kontextusban és bevezettem a kontrollált PFE (vagy CPFE) fogalmát, valamint ennek különböző relaxációit. Az új biztonság definíciókat kielégítő általános protokollokat mutattam és a relaxált követelmények alkalmazhatóságát egy a belső szorzatok számolására szolgáló konkrét protokoll vizsgálatával demonstráltam (részletekért lsd. a 2.2. alfejezetet valamint a disszertáció 4. fejezetét).

A következő téma, amivel foglalkoztam, a titkosított adatokhoz való rugalmas hozzáférés kezelés volt, pontosabban a hozzáférési jogosultságok visszavonása attribútumalapú titkosítás (ABE) esetén. A felhasználó-visszavonás nehézsége az ABE fő előnyében rejlik, méghozzá abban az extrém rugalmasságban, amivel felhasználói csoportokat lehet

azonosítani annak köszönhetően, hogy az egyes felhasználókat a rájuk jellemző nem egyedi attribútumaikkal írjuk le. Ugyanakkor, ezeket az attribútum-alapú leírásokat használva egy konkrét felhasználó azonosítása már nehézzé válhat, hiszen attribútumai más felhasználókkal közösek lehetnek. Ebből következik, hogy a rugalmas hozzáférés-kezelés és a hatékony felhasználó visszavonás együttes megvalósítása kompromisszumokat igénylő feladat. Erre a problémára javasoltam az első felhasználó-visszavonást támogató, elosztott módon működő ún. CP-ABE sémát és bizonyítottam a biztonságát (eredményeim részleteiért lsd. a 2.3. alfejezetet valamint a disszertáció 5. fejezetét).

Végül a disszertációm utolsó része a kereshető (szimmetrikus) titkosítás (SSE) eljárásoknak egy tervezési nehézségéhez kapcsolódik. A probléma, hogy a hatékony keresés lehetővé tételéhez (azaz az $O(n)$ keresési komplexitás lejjebb szorításához) a titkosított adatbázist valamilyen módon strukturálni kell. Ugyanakkor az új elemek hozzáadása az adatbázishoz különös figyelmet igényel, hiszen a struktúrának köszönhetően az ilyen frissítések információt szivárogtathatnak az adatbázisról. Az említett figyelem, jellemzően jelentős hatékonyságveszteséggel jár. Ebben a kontextusban vizsgáltam felül az ún. „forward index" megközelítést rávilágítva relevanciájára olyan esetekben, mikor a frissítések gyakoriak, ugyanakkor a keresések leszűkítők a teljes adatbázis egyes részeire. Az ehhez kapcsolódó eredményeimet a 2.4. alfejezetben (és a disszertáció 6. fejezetében) ismertetem.

Eredményeim alkalmazási lehetőségeit a 3. fejezetben foglalom össze.

2. Új eredmények

Ebben a fejezetben röviden ismertetem eredményeimet, melyek részletei megtalálhatók a disszertációmban.

2.1. Adatpiacok biztonsági analízise

A problémakör felmérése természetes kiindulópontja bármilyen rendszer biztonsággal kapcsolatos kérdéseinek vizsgálatakor. Mivel ismereteim szerint az adatpiacokat soha nem vizsgálták átfogóan ilyen szemszögből, ezért egy korábbi munkámban [C3] megvizsgáltam a piacok szereplőinek lehetséges kapcsolatát (a bizalom szemszögéből) és ezen kapcsolatok hatását a szükséges adatkezelési módszerekre.

0. Tézis: *Általános rendszermodellt javasoltam, ami leírja az adatpiacok résztvevőinek lehetséges érdekeit, szerepeit, és tevékenységét azzal a céllal, hogy az ezekből következő biztonsági célokat formalizálhassam. Megvizsgáltam az azonosított biztonsági célok különböző lehetséges együttesei által meghatározott szcenáriókat, majd ezeket összekapcsoltam a kriptográfia megfelelő ágaival.*

Elemzésemben az adatpiac résztvevői közti következő bizalmi lehetőségeket vizsgáltam. Az adattulajdonos vagy közvetlen hozzáférést enged adataihoz a brókernek, vagy szerepének megfelelően csak a metaadatokat ismerheti meg, minden mást legfeljebb rejtjelezett formában tárolhat. A szolgáltató vagy nyílt adatot vásárol, vagy olyan informáci-

ót, ami közvetve (valamilyen számítás bemeneteként) tartalmazza az adattulajdonos(ok) által biztosított adatokat. Azaz utóbbi esetben a szolgáltató a feldolgozatlan adathoz legfeljebb rejtjelezett formában juthat hozzá. A bróker és a szolgáltató kapcsolata összetettebb. Feltéve, hogy a szolgáltató számítási kapacitást is vásárolhat az adattal együtt, érdekében állhat a kiértékelt függvény, a felhasznált bemenet(ek), a bemenet(ek)hez tartozó metaadat(ok), valamint a számítás kimenetének titokban tartása is. A bróker szemszögéből a végrehajtott számítás lehet szabadon megválasztható vagy korlátozott. Utóbbi jelentése, hogy a bróker esetleg ellenőrizni szeretné, hogy az értékesített adatról milyen információt felfedését engedélyezi (a függvény kiértékelésén keresztül).

Ezen követelmények lehetséges kombinációi 2^7 db különböző szcenárióhoz vezetnek (lsd. az 1. táblázatot), melyek közt vannak ellentmondásosak, triviálisan megoldhatók, és kriptográfiai eszközöket igénylők. Ezen szcenáriók elemzését a disszertáció 3. fejezetében ismertetem, kiemelve számos nyitott kérdést, melyek további kutatás motivációjául szolgálhatnak.

2.2. Részinformáció szivárgás kontrolálása privát függvény kiértékelés esetén

A privát függvény kiértékelés (PFE) protokollok lehetővé teszik Aliz és Bob számára közös számítások biztonságos végrehajtását úgy, hogy Aliz a bemenetet Bob pedig a függvényt biztosítja ehhez. Feltesszük, hogy Bob hozzáfér a számítás kimenetéhez. A private function evaluation (PFE) biztonsági követelménye, hogy a protokoll futtatása egyik résztvevő számára se fedjen fel több információt a másik fél bemenetéről, mint amit az általa kapott kimenet már önmagában felfed. Világos, hogy a függvény védelme megakadályozza Alizt abban, hogy kontrollálhassa vagy akár csak kövesse, hogy Bob milyen mit tud meg az általa biztosított bemenetről. Ez a probléma a következő kérdéseket veti fel, melyekre [C2]-ben kerestem a válaszokat.

Elérhető, hogy egy PFE protokollban a bemenetet biztosító fél kizárhassa bizonyos érzékeny információk kiszivárgását a másik résztvevő felé, anélkül, hogy kiderülne mit szeretne elrejteni?
Van-e olyan kompromisszum a bemenet és a függvény védelmének mértéke között, ami hatékony protokollok megvalósítását teszi lehetővé, értelmes biztonsági garanciákkal?

1.1. Tézis: *Bevezettem a kontrollált PFE (controlled private function evaluation (CPFE)) fogalmát, mely egy definíciós keretrendszer segítségével garantálja, hogy tetszőleges részinformáció szivárgása bizonyíthatóan megelőzhető legyen miközben a kiértékelt függvény változó mértékben, de továbbra is privát maradhasson. A javasolt biztonság definíciók szimuláció-alapú biztonságot garantálnak kíváncsi, de őszinte („semi-honest") résztvevők esetén.*

A CPFE és relaxált változata a rCPFE formális biztonsági definíciója szerint, a résztvevők által kapott protokollüzeneteknek megkülönböztethetetleneknek kell lenniük ún.

					Megbízható adat bróker (hozzáférhet az adatokhoz)		Nem megbízható adat bróker (legfeljebb kriptoszöveghez fér hozzá)	
	függvény	bemenet(ek)	metaadata(ok)	kimenet	Szabad függvénykiértékelés (0)	Korlátozott függvénykiértékelés (1)	Szabad függvénykiértékelés (0)	Korlátozott függvénykiértékelés (1)
Megbízható szolgáltató (hozzáférhet az adatokhoz)	0	0	0	0	Bróker = Szolgáltató	Az adattulajdonos bízik a szolgáltatóban, aki így nyílt adatokat kap és ezen tetszőleges számítást végrehajthat, amit a bróker nem tud korlátozni	Input felfedése a brókernek ellentmond az adattulajdonos akaratának, aki elrejtené adatait a bróker elől	Az adattulajdonos bízik a szolgáltatóban, aki így nyílt adatokat kap és ezen tetszőleges számítást végrehajthat, amit a bróker nem tud korlátozni
	0	0	1	0	publikus bemenet⇔titkos metaadat			
	0	0	0	1	Függvény és bemenete meghatározza a kimenetet			
	0	0	1	1				
	0	1	0	0	Metaadata felfedi a bemenetet		A szolgáltató hozzáfér a nyers adatokhoz, így tetsz. függvényt kiértékelhet a bróker tudta nélkül	
	0	1	0	1				
	0	1	1	0	A szolgáltató hozzáfér a nyers adatokhoz, így tetsz. függvényt kiértékelhet a bróker tudta nélkül			
	0	1	1	1				
	1	0	0	0	Lokális számítás után a szolgáltató publikálja a kimenetet		Input felfedése a brókernek ellentmond az adattulajdonos akaratának, aki elrejtené adatait a bróker elől	
	1	0	0	1	A szolgáltató lokálisan végez számításokat			
	1	0	1	0	publikus bemenet⇔titkos metaadat			
	1	0	1	1				
	1	1	0	0	Metaadat felfedi a bemenetet		3.2a ábra publikus kimenettel	
	1	1	0	1			❷ – 3.2a ábra (2.3. fejezet)	
	1	1	1	0	A szolgáltató minden adatot letölt, lokálisan számol, eredményét publikálja		3.2b ábra publikus kimenettel	
	1	1	1	1	A szolgáltató minden adatot letölt, lokálisan számol		❸ – 3.2b ábra (2.4. fejezet)	
Nem megbízható szolgáltató (nyílt adatokhoz nem fér hozzá)	0	0	0	0	A kiszámítható függvények megszorítása nélkül a szolgáltató az identitásfüggvény kiértékelésével hozzájuthatna nyers adatokhoz, ami ellentmondana annak, hogy ilyet nem kaphat	Kiszervezett számítás függvény ellenőrzéssel	A kiszámítható függvények megszorítása nélkül a szolgáltató az identitásfüggvény kiértékelésével hozzájuthatna nyers adatokhoz, ami ellentmondana annak, hogy ilyet nem kaphat	Input felfedése a brókernek ellentmond az adattulajdonos akaratának, aki elrejtené adatait a bróker elől
	0	0	1	0		Publikus bemenet⇔titkos metaadat		
	0	0	0	1		Függvény és bemenete meghatározza a kimenetet		
	0	0	1	1				
	0	1	0	0		Metaadat felfedi a bemenetet		3.4a ábra publikus kimenettel
	0	1	0	1				3.4a ábra
	0	1	1	0		3.3a ábra publikus kimenettel		3.4 bábra publikus kimenettel
	0	1	1	1		3.3a ábra		3.4b ábra
	1	0	0	0		3.3b ábra publikus kimenettel		Input felfedése a brókernek ellentmond az adattulajdonos akaratának, aki elrejtené adatait a bróker elől
	1	0	0	1		❶ – 3.3b ábra (2.2. fejezet)		
	1	0	1	0		Publikus bemenet⇔titkos metaadat		
	1	0	1	1				
	1	1	0	0		Metaadat felfedi a bemenetet		3.4c ábra publikus kimenettel
	1	1	0	1				Fig. 3.4c
	1	1	1	0		3.3c ábra publikus kimenettel		3.4d ábra publikus kimenettel
	1	1	1	1		3.3c ábra		3.4d ábra

1. táblázat. Az azonosított szcenáriók összesítése, és felmerülő problémák ideális megoldási lehetősége (a hivatkozott ábrák megtalálhatóak a disszertációban). Az ellentmondásos helyzeteket szürke, a triviálisan megoldhatókat zöld, míg a kriptográfiai szempontból érdekes helyzeteket világos és sötét narancssárga szín jelöli. A számozott szcenáriók azok, melyek a saját új eredményeim szempontjából relevánsak.

PARAMÉTEREK: P_1, P_2 résztvevők, $\mathcal{F} = \{f : \mathcal{X} \to \mathcal{Y}\}$ determinisztikus függvények egy osztálya *[és $\kappa > k$ egész szám]*.

FUNKCIONALITÁS:
$x_1, \ldots, x_d \in \mathcal{X}$ és $\mathcal{F}_A \subset \mathcal{F}$ bemeneteken P_1-től; és $\mathcal{F}_B = \{f_1, \ldots, f_k\} \subset \mathcal{F}$, P_2-től:

- P_1 nem kap kimenetet, *[vagy P_1 kimenete $\mathcal{F}_R$, amire $\mathcal{F}_B \subset \mathcal{F}_R \subset \mathcal{F}$ és $|\mathcal{F}_R| = \kappa$]*
- P_2 kimenete $\{y'_{i,j} = f'_j(x_i)\}_{i\in[d],j\in[k]} \subset \mathcal{Y} \cup \{\perp\}$, ahol

$$f'_j(x_i) = \begin{cases} f_j(x_i) & \text{ha } f_j \notin \mathcal{F}_A \\ \perp & \text{egyébként.} \end{cases}$$

2. ábra. Az $\mathcal{F}_{\mathbf{CPFE}}$ ideális funkcionalitás, általánosan megfogalmazva több input és függvény egyidejü kiértékelésére. A szögletes zárójelbeli kiegészítés a relaxált változat (rCPFE) ideális funkcionalitását, $\mathcal{F}_{\mathbf{rCPFE}}$-t határozza meg, ami κ-anonimitás típusú függvény védettséget garantál [SS98].

szimulált üzenetektől. Szemléletesen, a biztonsági garanciát az adja, hogy a szimulált üzeneteket létrehozásához a protokoll nem, csak annak ideális funkcionalitása áll rendelkezésre (azaz az adott résztvevő be- és kimenetei). A CPFE és rCPFE definíciókhoz tartozó ideális funkcionalitások a 2 ábrán láthatók. A pontos definíciókat a disszertáció 4.3.1. fejezete tartalmazza.

1.2. Tézis: *Univerzális logikai hálózatokra (UC) és biztonságos kétszereplős számítási protokollokra (2PC) támaszkodva javasoltam a CPFE definíció általános megvalósítását, melynek biztonsága kizárólag a felhasznált eszközök biztonságán múlik.*

A disszertáció 4.3.2. fejezetében javasolt protokoll, koncepcionálisan egyszerű és demonstrálja a CPFE definíció megvalósíthatóságát. Alapötlete, hogy a számítás bemenetét szolgáltató résztvevő függvényre vonatkozó megszorításai kezelhetők egy extra bemenetként, melyet egy 2PC protokollnak ad át. Ugyanakkor, a protokoll rávilágít a definíció relaxálásának fontosságára, annak érdekében, hogy hatékonyabb protokollokat kaphassunk.

1.3. Tézis: *Olyan protokollt javasoltam két-szereplős biztonságos függvénykiértékelésre, mely lehetővé teszi a protokollüzenetek újrahasznosítását, abban az esetben, ha több függvénykiértékelést is végrehajtanak a résztvevők. Ennek eredménye, hogy ugyanazon függvénye(ek) kiértékelése több, pl. d darab bemeneten, d-vel arányos additív többletmunkát igényel a kommunikációs és online számítási igény esetében is. Ezzel szemben, hagyományos PFE esetén ugyanez multiplikatív többletmunkával jár. A protokollról bizonyítottam, hogy mindaddig teljesíti a rCPFE biztonsági követelményeket, míg a felhasznált primitívek teljesítenek standard biztonsági követelményeket.*

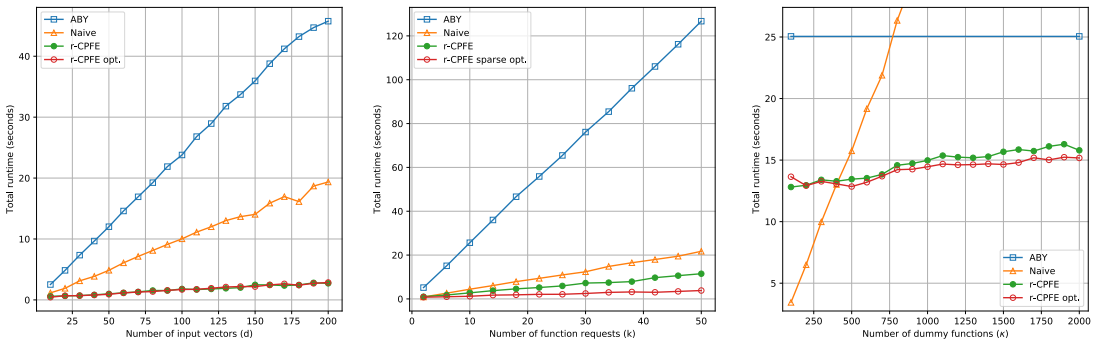
Az általános rCPFE megvalósítás alapötlete, hogy Aliz titkosított formában elküldheti a felhasználásra szánt bemeneteket Bobnak, ha azok dekódolhatóságát megfelelően tudja szabályozni. A funkcionális titkosítás (FE) éppen erre ad lehetőséget, azzal, hogy adott függvényhez generált titkos kulcs, a dekódolásba integráltan teszi lehetővé a függvény kiértékelését. Azaz egy x értéket titkosító kriptoszöveget az f függvényhez tartozó ún. funkcionális titkos kulccsal dekódolva éppen $f(x)$ értékét ismerhetjük meg, mást azonban nem. Az FE alkalmazásának kihívása, hogy valamilyen módon Aliznak elérhetővé kell tennie Bob számára a megfelelő funkcionális kulcsot, melyre egy ún. oblivious transfer (OT) protokoll ad lehetőséget. A protokoll biztonságáról és hatékonyságáról szóló pontos állítások megtalálhatók a disszertáció 4.3.2. Tételében és a 4.3.2.1. valamint a 4.3.2.2. Következményben a biztonság bizonyításával együtt.

1.4. Tézis: *A javasolt általános rCPFE protokoll praktikus belső szorzatok kiértékelésére. Ezt demonstrálja a koncepció igazolására készített és optimalizált eljárásokkal bővített implementáció, valamint ennek összehasonlítása a legkorszerűbb, biztonságos aritmetikai belső szorzat számításokat lehetővétevő protokollal [DSZ15].*

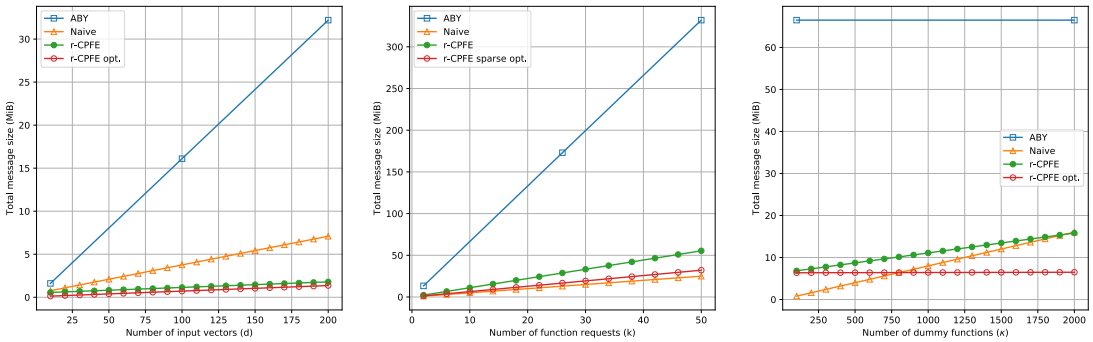
[ALS16] k-NA-SIM biztonságú functional encryption (FE) konstrukciója és [Tze04] „semi-honest", „1-ből κ" OT protokolljának felhasználásával a javasolt általános rCPFE protokoll egy konkrét megvalósítását kapjuk belső szorzatok számolására, melynek biztonságának alapja a döntési Diffie–Hellman feltevés (DDH). Ezt a konkrét protokollt két további optimalizációs lehetőséggel együtt vizsgáltam: az egyik előszámítások végrehajtását teszi lehetővé, míg a másik azt képes kihasználni ha a bemeneti vektorok egyikéről tudjuk, hogy ritka. Ezen protokollok teljesítménye egy naiv OT-alapú megoldással és az etalonnak tekinthető ABY keretrendszerrel [DSZ15] lett összehasonlítva. Az eredmények a 3 ábrán láthatók, illetve a disszertáció 4.4. fejezetében részletesebben is megtalálhatók.

2.3. Felhasználóvisszavonás elosztott attribútum-alapú titkosítás esetén

Az attribútum-alapú titkosítás (ABE) célja, hogy egyszerre több címzettnek küldhessünk titkosított üzenetet, mindezt úgy, hogy a dekódolásra pontosan azok legyenek csak képesek, akik megfelelnek bizonyos kritériumoknak. Az ún. CP-ABE sémákban, a felhasználókat leíró attribútumaik alapján titkos kulcsaikat (és a megfelelő publikus



(a) $\ell = 100, k = 1, \kappa = 1000$ (b) $\ell = 1000, d = 10, \kappa = 100$ (c) $\ell = 1000, d = 100, k = 1$



(d) $\ell = 100, k = 1, \kappa = 1000$ (e) $\ell = 1000, d = 10, \kappa = 100$ (f) $\ell = 1000, d = 100, k = 1$

3. ábra. A javasolt protokollok és az ABY keretrendszer [DSZ15] teljes futásidejének (3a–3c) és aggregált kommunikációs költségének (3d–3f) összehasonlítása (ℓ a vektor dimenziót, d és k a bemeneti és „függvény vektorok” számát, míg κ az ún. „báb vektorok” számát jelöli). A mérések egy felhasználói laptopon készültek, melynek fontosabb jellemzői: 2.60GHz Intel® Core™ i7-6700HQ CPU és 4GB RAM.

kulcsokat) egy „attribútum hatóság” állítja, míg a kriptoszövegek tartalmazzák az attribútumokra vonatkozó, dekódoláshoz szükséges kritériumokat, melyeket a küldő határoz meg. Adott kriptoszöveg akkor és csak akkor dekódolható, ha a dekódoló attribútumai kielégítik a kriptoszövegben adott feltételt. Az ABE előnye, hogy biztonságos adatmegosztást tesz lehetővé, anélkül, hogy a küldőnek előre ismernie kellene a később dekódolásra képes felhasználókat, ami lehetővé teszi a titkosított adatok rugalmas kezelhetőségét.

Természetesen a rugalmas felhasználóazonosításnak ára van, amit akkor kell megfizetnünk, amikor egy konkrét felhasználó azonosítása válik szükségessé. Tipikus példája ennek, egy felhasználó jogosultságainak visszavonása. Ennek biztosítása a mindennapi használatban elengedhetetlen, hiszen váratlan események bekövetkezése befolyásolhatja a felhasználói jogokat, amit a kriptorendszernek is követnie kell. Ilyen események lehetnek pl. az elbocsájtás, rosszindulatú tevékenység feltárása, stb. Mivel ABE rendszerekben különböző felhasználók gyakran azonos funkcionalitású (azaz azonos attribútumoknak

megfeleltethető) kulcsokat birtokolnak, ezért a felhasználó visszavonás különösen nehéz problémát jelent.

2.1. Tézis: *Biztonsági modellt javasoltam elosztott (több attribútum hatósággal rendelkező) és identitásalapú felhasználó-visszavonást lehetővé tevő CP-ABE kriptorendszerek biztonságának elemzésére.*

[C5] javasolta az első identitásalapú felhasználó-visszavonást lehetővé tevő CP-ABE rendszert, melyben több hatóság is előállíthatja az attribútum kulcsokat. A rendszer biztonságának bizonyításához szükséges egy modell, ami leírja a támadó lehetőségeit. Ebben az ún. játék alapú megközelítést követtem, ami a biztonságot egy kihívó ($\mathcal{C}$) és támadó algoritmusok ($\mathcal{A}$) közti játék felhasználásával ragadja meg. A játékban feltesszük, hogy $\mathcal{A}$ statikusan korrumpálhat attribútum hatóságokat, adaptív kulcskéréseket küldhet a kihívónak. Biztonság definícióm azt a szélsőséges esetet vizsgálja, amikor az összes visszavont jogosultságú felhasználó közreműködik egy támadásban. Szemléletesen, a támadó meghatározhatja, hogy mely hatóságok kulcsaihoz, mely identitású felhasználók paramétereihez, milyen attribútum titkos kulcsokhoz szeretne hozzáférni, és hogy milyen üzenetpárból válaszon számára a kihívó egy üzenetet, melyet titkosít, és amiről el kell döntenie, hogy a pár melyik elemének kriptoszöveg változatát láthatja. Az egyetlen természetes megkötés, hogy a támadó számára rendelkezésre álló információk ne tehessék lehetővé a *legitim* dekódolást. A biztonsági játékot akkor nyeri $\mathcal{A}$, ha a kihívás során kapott kriptoszövegről meg tudja állapítani, hogy melyik általa választott nyílt üzenetet titkosítja. A formális biztonsági játék a következő körökből áll:

Setup. $\mathcal{C}$ a séma setup algoritmusának futtatásával előállítja a GP globális paramétereket. $\mathcal{A}$ meghatározza az $AA' \subseteq AA$ korrupt hatóságok halmazát, majd a hatóságok setup algoritmusával előállítja a hatóságok publikus és titkos kulcsait. Az őszinte attribútum hatoságok ($AA \setminus AA'$) és a központi identitás ellenőrző hatóság számára $\mathcal{C}$ generálja a szükséges kulcsokat a megfelelő algoritmusok futtatásával, majd az így kapozz publikus kulcsokat elküldi $\mathcal{A}$-nak.

Kulcs-kérés fázis. $\mathcal{A}$ adaptív titkos kulcs kéréseket küld GID_k (a k. kérést jelölő) globális azonosítójú korrumpált felhasználó nevében $\mathcal{C}$-nek, aki a megfelelő identitás kulcsokkal válaszol $\mathcal{A}$-nak. Jelölje UL az $\mathcal{A}$ által lekért összes GID_k halmazát. $\mathcal{A}$ attribútum kulcs kéréseket is küld $\mathcal{C}$-nek (i, GID_k) párok elküldésével, ahol i olyan attribútumot jelöl, mely őszinte hatósághoz tartozik. $\mathcal{C}$ ismét a megfelelő attribútum titkos kulcsokkal válaszol.

Kihívás. $\mathcal{A}$ két üzenetet, $\mathfrak{m}_0, \mathfrak{m}_1$-et küld $\mathcal{C}$-nek, $RL \subseteq UL$ visszavont felhasználó azonosítók listájával, és egy $\mathcal{P}$ hozzáférési követelményrendszerrel együtt.

RL-nek és $\mathcal{P}$-nek a következő követelményeket kell teljesíteniük. Jelölje V az vizsgált rendszerben használt attribútumoknak azon részhalmazát, amik korrupt hatóságokhoz tartoznak. Minden $GID_k \in UL$ esetén jelölje V_{GID_k} azon i attribútumok részhalmazát, amelyekre $\mathcal{A}$ (i, GID_k) kérést küldött. $GID_k \in UL \setminus RL$ esetén

$V \cup V_{GID_k}$-beli attribútumok nem teljesíthetik a $\mathcal{P}$ követelményt, míg $GID_k \in RL$ esetén, csak V-beli attribútumok nem teljesíthetik $\mathcal{P}$-t.

A fentieken túl $\mathcal{A}$ átadja $\mathcal{C}$-nek a $\mathcal{P}$ által használt, korrumpált hatóságokhoz tartozó publikus attribútum kulcsokat is.

$\beta \in (0,1)$ random érték sorsolása után, $\mathcal{C}$ titkosítja M_β-t a $\mathcal{P}$ követelmények és a RL visszavonási lista valamint a szükséges publikus attribútum kulcsok felhasználásával.

2. kulcs-kérés fázis. $\mathcal{A}$ további (i, GID_k) attribútum kéréseket küldhet $\mathcal{C}$-nek, melyekre mindaddig választ kap, amíg azok nem sértik az RL listára és $\mathcal{P}$ követelményekre fent adott megszorításokat.

Tipp. $\mathcal{A}$ egy β' megoldást küld a kihívásra, melyet $\mathcal{A}$ nyer, ha $\beta' = \beta$. A támadó játékbeli előnyét a következő valószínűséggel definiáljuk: $\mathbb{P}(\beta' = \beta) - \frac{1}{2}$.

1. Definíció. *Azt mondjuk, hogy egy identitásalapú felhasználó visszavonást támogató elosztott CP-ABE kriptorendszer biztonságot nyújt választott nyílt szöveg alapú támadások és a hatóságok statikus korrupciója ellen, tetszőleges, a biztonsági paraméter valamely polinomjánál nem nagyobb méretű RL visszavont felhasználói lista esetén, bármely polinom időben futó $\mathcal{A}$ támadó algoritmus ellen, ha a fent definiált biztonsági játékban legfeljebb elhanyagolható előnyre tud szert tenni.*

2.2. Tézis: *Identitásalapú felhasználó visszavonást támogató elosztott CP-ABE kriptorendszert javasoltam, melynek biztonságát az általános bilineáris csoport illetve a random orákulum modellekben bizonyítottam.*

A [C5, J2] publikációkban egy korábbi megoldás a [LW11] továbbfejlesztéseként javasoltam konstrukciót az említett feltételeket teljesítő kriptorendszerre. Megoldásom fő előnye a korábban elterjedt attribútum-alapú felhasználó visszavonással összehasonlítva, hogy direkt visszavonást tesz lehetővé és nem érinti az egyes attribútum kulcsokat, amiket korábban frissíteni kellet minden olyan felhasználó esetén, aki a visszavont felhasználóval közös attribútummal rendelkezett. Másrészt a visszavonási jog közvetlenül a kódoló kezébe került összhangban a hozzáférési követelmények meghatározásával.

Az említett célok megvalósításakor, más környezetben megvalósított felhasználó visszavonással kapcsolatos technikákat is felhasználtam [LSW10]. Az alapötlet egy olyan titokmegosztás használata volt a kriptoszövegek konstruálásakor, aminek célja, hogy a dekódoláshoz szükséges legyen a titok rekonstruálása, ennek feltétele azonban az, hogy a dekódoló globális azonosítója ne szerepeljen a kriptoszövegbe ágyazott RL listán. A megvalósításhoz a következő kihívásokat kellett megoldani: Először is elengedhetetlen volt garantálni, hogy a dekódoló az RL lista minden elemével összehasonlítsa a saját azonosítóját, még akkor is, ha attribútum kulcsai lehetővé tennék a dekódolást. Másodszor biztosítani kellett, hogy a dekódoló azonosítójának RL bármely elemével való egyezése esetén az érintett felhasználó ne juthasson hozzá a dekódoláshoz szükséges információhoz. És végül a visszavont felhasználók együttműködésének hasznosságát kellett

meggátolni. Ezen problémák megoldása valamint a javasolt konstrukció részletes leírása és a formális biztonság bizonyítás megtalálhatók a disszertáció 5.3–5.4. fejezeteiben.

2.4. Kereshető titkosítás adatbázisok korlátozott kereséséhez

A kereshető szimmetrikus titkosítás lehetővé teszi, hogy titkosított dokumentumok (vagy tetszőleges adat) mellé titkosított kulcsszavakat (metaadatot) csatoljunk. Ez utóbbiak közt dekódolás nélkül kereshet egy nem megbízható fél (pl. egy szerver) egy erre a célra, a titkosításhoz használt titkos kulcs felhasználásával készített ún. „trapdoor" segítségével.

Az SSE két természetes megközelítése ismert, melyeket előre- és invertált indexelésnek nevezünk. Az első esetben a titkosított adathoz csatoljuk a kereshető kulcsszavak valamely egyirányú leképezéssel kapott képét. Ez lineáris keresési komplexitáshoz vezet (a dokumentumok számában), hisz a szervernek szekvenciálisan kell a trapdoort a kulcsszavak képével „összehasonlítania". Az invertált index egy szofisztikáltabb elrendezést jelent, ahol általában a kulcsszavak képe alapján rendezik a dokumentum azonosítókat a kulcsszavak számában logaritmikus lépésszámú keresést téve lehetővé. Ez az egyértelmű előny tette egyeduralkodóvá az utóbbi megközelítést az SSE tervezésben [PCY+17].

Ugyanakkor, az így kapott megoldások hátránya, hogy szinte statikus adatbázisok helyett nagyon gyorsan bővülő adathalmaz esetén a komplex adatstruktúrák kezelése kihívást jelent. Új dokumentum hozzáadása esetén ugyanis a strukturált tárolásból adódó információszivárgás megakadályozása összetett megoldásokat igényel (lsd. a 2 táblázatot részletekért). [C4, J1] és a disszertáció 6. fejezete a következő kérdéseket vizsgálja:

Mi a legkedvezőbb SSE eljárás olyan esetekben, amikor a titkosított adatbázis gyorsan bővül, ugyanakkor a teljes adatbázis helyett annak részhalmazában kell csak keresnünk a titkosított dokumentumokat?

Az általános esetekkel ellentétben, a keresési sebességre optimalizált invertált index megközelítés kevésbé kifizetődő ilyenkor és a kevéssé vizsgált szekvenciális keresés jelentheti a megoldást.

3.1. Tézis: **IND-CKA2** *típusú biztonsági definíciót javasoltam előre indexelt SSE kriptorendszerek biztonságának vizsgálatára.*

Az **IND-CKA2**[4] biztonsági modellt **IND-CKA2** definiálta annak az intuíciónak a formalizálására, hogy egy SSE sémával titkosított adatbázis és az ezen végrehajtott keresések együttesen nem fedhetnek fel több információt a rejtjelezett adatokról, mint amennyit a keresési mintázat és a keresések kimenete felfed. Az általam javasolt definíció is ezt az intuíciót formalizálja, de az előre indexelt keresésre átültetve.

A biztonsági játékban az $\mathcal{A}$ támadó algoritmus feladata az általa meghatározott adatbázisok egyikének felismerése, melyet a kihívó titkosított számára. Megjegyezzük, hogy az előre indexelés sajátossága, hogy a játékban a titkosított adatbázis kriptoszövegek sorrendje is segíthetné $\mathcal{A}$t, míg a valóságban ilyen probléma nem merül fel. Ennek

[4] megkülönböztethetetlenség adaptívan választott kulcsszó támadás esetén

kiküszöbölése miatt a kihívó minden esetben egy random permutációt hajt végra az adatbázison a titkosítás előtt. A támadót segíti, hogy a játék során adaptív trapdoor kérésekre kap válaszokat, azzal az egy megkötéssel, hogy így végrehajtható keresések nem szeparálhatják a kihívásban szereplő adatbázisokat (hiszen a keresések kimenetén kívüli információszivárgást szeretnénk elkerülni).

Az egyszerűség kedvéért feltesszük, hogy minden dokumentumhoz egyetlen kulcsszó tartozik, ez azonban könnyen általánosítható. A formális biztonság definíció tehát a következő:

2. Definíció (**IND-CKA2** biztonság)**.** *Legyen SSE = (**Setup**, **Enc**, **TrpdGen**, **Dec**, **Test**) egy szimmetrikus-kulcsú kereshető titkosító eljárás, $\lambda \in \mathbb{N}$ a biztonsági paraméter, és $\mathcal{A} = (\mathcal{A}_0, \ldots, \mathcal{A}_{q+1})$ nem uniform támadó algoritmus. Tekintsük a 4. ábrán látható* $\mathbf{IND\text{-}CKA2}_{\mathbf{SSE},\mathcal{A}}(\lambda)$ *kísérletet, azzal a megkötéssel, hogy D^0-ban és D^1-ben a támadó által kért trapdoorok azonos számú találatot adnak, azaz*

$$\#\{i|\hat{w}_j^0 = w_i^0 \ \forall j \in [k]\} = \#\{i|\hat{w}_j^1 = w_i^1 \ \forall j \in [k]\}$$

minden $k = 1, \ldots, q$ esetén, ahol q a λ biztonsági paraméter valamely polinomja.

$\mathbf{IND\text{-}CKA2}_{\mathbf{SSE},\mathcal{A}}(\lambda)$ Biztonsági játék

$\mathsf{sk} \leftarrow_\$ \mathbf{SSE.Setup}(1^\lambda)$
$b \leftarrow_\$ \{0,1\}$
$(\mathsf{state}_{\mathcal{A}_0}, D^0, D^1) \leftarrow \mathcal{A}_0(1^\lambda)$
parse D^b as $\{(m_1^b, w_1^b), \ldots, (m_n^b, w_n^b)\}$
for $1 \le j \le n$,
  $C_i^b \leftarrow_\$ \mathbf{SSE.Enc}(\mathsf{sk}, m_i^b, w_i^b)$,
$C^b := (C_{\pi_1}^b, \ldots, C_{\pi_n}^b)$ valamilyen π random permutációra,
for $1 \le j \le q$,
  $(\mathsf{state}_{\mathcal{A}_j}, \hat{w}_j^0, \hat{w}_j^1) \leftarrow \mathcal{A}_j(\mathsf{state}_{\mathcal{A}_{j-1}}, C^b, \{T_i^b\}_{i\in[j]})$
  $T_j^b \leftarrow_\$ \mathbf{SSE.TrpdGen}(\mathsf{sk}, \hat{w}_j^b)$
$b' \leftarrow \mathcal{A}_{q+1}(\mathsf{state}_{\mathcal{A}_q}, C^b, \{T_j\}_{i=1,\ldots,q})$
return $b = b'$

4. ábra. **IND-CKA2** biztonsági játék előre indexelt searchable symmetric-key encryption (SSE) sémákhoz.

Azt mondjuk, hogy egy előre indexelt SSE séma **IND-CKA2** *biztonságú, ha tetszőleges polinom idejű $\mathcal{A} = (\mathcal{A}_0, \ldots, \mathcal{A}_{q+1})$ támadó esetén*

$$\Pr(\mathbf{IND\text{-}CKA2}_{\mathbf{SSE},\mathcal{A}}(\lambda) = 1) \le \frac{1}{2} + \mathsf{negl}(\lambda).$$

3.2. Tézis: **IND-CPA** *biztonságú szimmetrikus-kulcsú rejtjelezés és* **EU-CMA** *biztonságú üzenethitelesítés felhasználásával konstruált* **IND-CKA2** *biztonságú SSE sémát javasoltam, melynek biztonságát a standard modellben az ún. szimmetrikus külső Diffie–Hellman (SXDH) feltevésre alapozva bizonyítottam.*

A konstrukció egyik előnye az egyszerűség. A kulcsszavakhoz tartozó kriptoszövegek és a trapdoor-ok szimmetrikus módon konstruáltak: mindkettő az adott kulcsszó randomizált MAC függvénye, viszont különböző csoportokban reprezentálva. Az azonosság tesztelését egy bilineáris művelet teszi lehetővé, mely a különböző csoportok felett értelmezett, így garantálva, hogy az összehasonlítás csak kriptoszöveg és trapdoor között lehetséges, azonos típusú elemek közt azonban nem. Az algoritmusok további részleteit a disszertáció 6.3.3. fejezete tartalmazza, míg a 6.4.1. tétel és bizonyítása a kostrukció biztonságát demonstrálja az SXDH feltevés fennállása mellett. A 2. táblázat a javasolt séma és más megoldások összehasonlítását mutatja.

Séma	**Modell**	**Biztonság**	**Fw/Bw Privacy**[5]	**Frissítés komplexitás**	**Frissítés biztonság**	**Keresés komplexitás**
[SWP00]	Standard	**IND-CPA**	× / ×	$O(b)$	×	$O(n \cdot b)$
[vLSD+10]	Standard	**IND-CKA2**	× / ×	$O(w_D)^*$	×	$O(\log W)$
[KPR12]	ROM	**CKA2**	× / ×	$O(w_D)$	×	$O(n_w)$
[KP13]	ROM	**CKA2**	× / ×	$O(\log n)^*$	✓	$O(n_w \log n)$
[CJJ+14]	ROM	**CKA2**	× / ×	$O(w_D + W \log n)$	×	$O(n_w + a + d)$
[SPS14]	ROM	**CKA2**	✓ / ×	$O(w_D \log(nW))^*$	✓	$O(n_w + d)$
[HK14]	ROM	**CKA2**	× / ×	$O(nw_D/W)^{**}$	×	$O(nw_D/W)^{**}$
[YG15]	ROM	**CKA2**	✓ / ✓	$O(W)$	✓	$O(W)$
[Gaj16]	Standard	**IND-CKA2**	× / ×	$O(w_D \cdot W)$	×	$O(\log n)$
[KKL+17]	ROM	**CKA2**	✓ / ×	$O(w_D)^*$	✓	$O(n_w)^*$
Saját	Standard	**IND-CKA2**	✓ / ✓	$O(w_D)$	✓	$O(n \cdot w_D)$

2. táblázat. Dinamikus SSE sémák és a saját eredmények összehasonlítása (n jelöli a dokumentumok számát, w_D a dokumentumonkénti kulcsszó számot, W a különböző kulcsszavak számát az adatbázisban, n_w a w kulcsszót tartalmazó dokumentumok száma az adatbázisban, a az adatbázihos hozzáadott összes új elem száma, d a törölt elemek száma, végül b a titkosított dokumentumok bithosszúsága). A csillaggal jelölt esetekben a frissítéshez interakció szükséges a kliens és a szerver között, míg a dupla csillag jelölés amortizált komplexitást jelöl.

3. Az eredmények alkalmazása

Az eredményeim rövid ismertetését, azok egy-egy adatpiacokhoz kapcsolódó alkalmazásának rövid ismertetésével zárom. További alkalmazási lehetőségeket a disszertáció 4.1.2., 5.1.2. és 6.1.2. fejezetei tartalmaznak. A szcenáriók számozása az 1. táblázatbeli szcenáriókra utal.

[5] A forward/backward privacy jelentése, hogy adott trapdoor segítségével csak a trapoor generálása előtt/után az adatbázishoz adott dokumentumok kulcsszavai kereshetők.

❶. **Szenárió:** Feltételezzük, hogy adattulajdonosok vektor formátumú lokáció-alapú információkat biztosítanak az adatbrókernek. A vektorelemek adott pozíciókban mért értékeknek feleljenek meg. Különösen fontosak az ilyen adatok lokáció-alapú szolgáltatások esetén ha a szolgáltató nem rendelkezik saját infrastruktúrával az adatok gyűjtésére. Ilyen szolgáltatók egyszerű statisztikai számításokhoz belső szorzat kiértékelést vásárolhatnak az adatbrókertől, azonban eközben a saját súlyvektoruk elrejtése nélkül felfedhetnék felhasználóik adatait. Ugyanakkor a bróker (vagy az adattulajdonos) érdekében állhat egyes pozíciók adatainak védelme vagy a bróker a statisztikában felhasznált adatmennyiséghez kötheti a szolgáltatás árát (esetleg eltérő árat állapíthat meg különböző pozícióban lévő értékek használatáért). Ezen célok együttesen elérhetők, ha a bróker a javasolt rCPFE protokoll segítségével kontrollálja a kiszámítható belső szorzatokat.

❷. **Szenárió:** Adattulajdonosok egyebek közt CP-ABE segítségével kontrollálhatják az adataikhoz való hozzáférést (pl. ha a brókerben nem bíznak meg). Helyzetéből adódóan a bróker ideális módon kezelheti a nála regisztrált szolgáltatók identitáskulcsait és a rendszer *RL* felhasználó visszavonási listáját. Az attribútum hatóságok szerepét olyan, az adatpiactól független entitások tölthetik be, melyekben az adattulajdonosok megbízhatnak (pl. ellenőrző szervek, fogyasztóvédelmi szervezetek). A javasolt CP-ABE séma előnye teljesen az adattulajdonos kezébe adja az adatai feletti kontrollt és anélkül határozhatja meg, kinek adja el adatait, hogy konkrét szolgáltatókat kellene meghatároznia. Ehelyett elég ha a preferált szolgáltatásokat nyújtók attribútumaira vonatkozó követelményeket beépíti a rejtjelezett adatba.

❸. **Szenárió:** Feltételezzük, hogy az adatbróker által tárolt metaadatok több rekordból állnak, melyek granuralitása eltérő. Ezért az általánosabbak nyilvánosak, míg a részleteket tartalmazók SSE segítségével titkosítottak. Ez esetben, a brókernek a tárolt adatoknak csak egy részhalmazában kell keresnie a szolgáltató által használni kívánt, titkosított adatokat, ami megtehető a javasolt SSE sémával. Ehhez a ❷. problémára adott megoldást azzal kell kiegészítenünk, hogy az adattulajdonos a trapdoor generálásához szükséges SSE kulcsot is rejtjelezze CP-ABE segítségével. Így ha egy szolgáltató jogosult ennek dekódolására, akkor a bróker adatbázisában anélkül tud keresni az adott adattulajdonos adatai között, hogy a brókernek felfedné pontosan mire kíváncsi. Ezzel megoldást kapunk a szolgáltató és adattulajdonos által is megbízhatatlannak ítélt bróker problémájára, anélkül, hogy le kellene mondanunk a bróker adattárolásban betöltött szerepéről.

Publikációk listája

Konferencia és workshop közlemények

[C1] Gergely Biczók, Máté Horváth, Szilveszter Szebeni, István Lám and Levente Buttyán. The cost of having been pwned: A security service provider's perspective. *The 3rd International Workshop on Emerging Technologies for Authorization and Authentication (Co-Located with ESORICS 2020) – ETAA 2020.*

[C2] Máté Horváth, Levente Buttyán, Gábor Székely and Dóra Neubrandt. There Is Always an Exception: Controlling Partial Information Leakage in Secure Computation. *J. H. Seo (Ed.): Information Security and Cryptology - ICISC 2019, LNCS 11975, pp. 133–149, 2020.*

[C3] Máté Horváth, Levente Buttyán. Problem Domain Analysis of IoT-Driven Secure Data Markets. In: E. Gelenbe et al. (eds) *Security in Computer and Information Sciences. Euro-CYBERSEC 2018. Communications in Computer and Information Science*, vol 821. pp. 57–67, Springer, 2018.

[C4] Máté Horváth, István Vajda. Searchable symmetric encryption: Sequential scan can be practical. *2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp 1–5, 2017.

[C5] Máté Horváth. Attribute-Based Encryption Optimized for Cloud Computing. G.F. Italiano et al. (eds), *SOFSEM 2015: Theory and Practice of Computer Science – 41st International Conference on Current Trends in Theory and Practice of Computer Science, Pec pod Sněžkou, Czech Republic, January 24–29, 2015. Proceedings*, *Lecture Notes in Computer Science* vol. 8939, pp. 566–577, Springer, 2015.

[C6] Máté Horváth. Private Key Delegation in Attribute-Based Encryption. *Mesterpróba – Conference for last year MSc and first year PhD students*, pp. 21–24, 2015.

Folyóiratcikkek

[J1] Máté Horváth, István Vajda. Searchable Symmetric Encryption for Restricted Search. *Journal of Communications Software and Systems*, 14(1):104–111, 2018.

[J2] Máté Horváth. Attribute-Based Encryption Optimized for Cloud Computing. *Infocommunications Journal*, 7(2):1–9, 2015.

Könyv

[B1] Máté Horváth, Levente Buttyán. Cryptographic Obfuscation: A Survey. *Springer Briefs in Computer Science, ISBN 978-3-319-98040-9.* Springer, 2020. Manuscript is available here: `http://eprint.iacr.org/2015/412`.

Hivatkozások

[ALS16] Shweta Agrawal, Benoît Libert, and Damien Stehlé. Fully secure functional encryption for inner products, from standard assumptions. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016, Proceedings, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 333–362. Springer, 2016.

[Bar16] Boaz Barak. Lecture notes from the Cryptography course at Harvard University, Spring 2016. https://intensecrypto.org/public/lec_17_SFE.html, Accessed 4. October 2020.

[CJJ+14] David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit S. Jutla, Hugo Krawczyk, Marcel-Catalin Rosu, and Michael Steiner. Dynamic searchable encryption in very-large databases: Data structures and implementation. In *21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014*, 2014.

[CMM+20] Gabriella Cattaneo, Giorgio Micheletti, Chrysoula Mitta, Mike Glennon, and Carla La Croce. *The European data market monitoring tool, Key facts & figures, first policy conclusions, data landscape and quantified stories: d2.9 final study report.* Publications Office of the EU, July 2020.

[Dat] Data Market Austria Project. https://datamarket.at/en/, Accessed 4. October 2020.

[Dat17] Datum Network GmbH. Datum Network - The decentralized data marketplace (White Paper V15). Technical report, Datum Network GmbH., 2017. https://datum.org/, Accessed 4. October 2020.

[DSZ15] Daniel Demmler, Thomas Schneider, and Michael Zohner. ABY - A framework for efficient mixed-protocol secure two-party computation. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015*. The Internet Society, 2015.

[EN16] Steven Englehardt and Arvind Narayanan. Online tracking: A 1-million-site measurement and analysis. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 1388–1401. ACM, 2016.

[Gaj16] Sebastian Gajek. Dynamic symmetric searchable encryption from constrained functional encryption. In *Topics in Cryptology - CT-RSA 2016 - The Cryptographers' Track at the RSA Conference 2016, San Francisco, CA, USA, February 29 - March 4, 2016, Proceedings*, pages 75–89, 2016.

[HK14] Florian Hahn and Florian Kerschbaum. Searchable encryption with secure and efficient updates. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, AZ, USA, November 3-7, 2014*, pages 310–320, 2014.

[IOT] IOTA Data Marketplace. https://data.iota.org/, Accessed: 4. October 2020.

[KKL+17] Kee Sung Kim, Minkyu Kim, Dongsoo Lee, Je Hong Park, and Woo-Hwan Kim. Forward secure dynamic searchable symmetric encryption with efficient updates. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, pages 1449–1463. ACM, 2017.

[KP13] Seny Kamara and Charalampos Papamanthou. Parallel and dynamic searchable symmetric encryption. In *Financial Cryptography and Data Security - 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers*, pages 258–274, 2013.

[KPR12] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. Dynamic searchable symmetric encryption. In *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*, pages 965–976, 2012.

[LSW10] Allison Lewko, Amit Sahai, and Brent Waters. Revocation systems with very small private keys. In *IEEE Symposium on Security and Privacy*, pages 273–285, 2010.

[LW11] Allison Lewko and Brent Waters. Decentralizing attribute-based encryption. In *Advances in Cryptology–EUROCRYPT 2011*, pages 568–588. Springer, 2011.

[Oce] Ocean Protocol Foundation Ltd. A decentralized data exchange protocol to unlock data for artificial intelligence (technical primer). https://oceanprotocol.com/, Accessed 4. October 2020.

[PCY+17] Geong Sen Poh, Ji-Jian Chin, Wei-Chuen Yau, Kim-Kwang Raymond Choo, and Moesfa Soeheila Mohamad. Searchable symmetric encryption: Designs and challenges. *ACM Comput. Surv.*, 50(3):40:1–40:37, 2017.

[SPS14] Emil Stefanov, Charalampos Papamanthou, and Elaine Shi. Practical dynamic searchable encryption with small leakage. In *21st Annual Network and Distributed System Security Symposium, NDSS 2014, San Diego, California, USA, February 23-26, 2014*, 2014.

[SS98] Pierangela Samarati and Latanya Sweeney. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression. techreport, SRI-CSL-98-04, SRI Computer Science Laboratory, 1998. Technical report.

[SWP00] Dawn Xiaodong Song, David Wagner, and Adrian Perrig. Practical techniques for searches on encrypted data. In *2000 IEEE Symposium on Security and Privacy, Berkeley, California, USA, May 14-17, 2000*, pages 44–55, 2000.

[Tze04] Wen-Guey Tzeng. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters. *IEEE Trans. Computers*, 53(2):232–240, 2004.

[vLSD+10] Peter van Liesdonk, Saeed Sedghi, Jeroen Doumen, Pieter H. Hartel, and Willem Jonker. Computationally efficient searchable symmetric encryption. In *Secure Data Management, 7th VLDB Workshop, SDM 2010, Singapore, September 17, 2010. Proceedings*, pages 87–100, 2010.

[YG15] Attila Altay Yavuz and Jorge Guajardo. Dynamic searchable symmetric encryption with minimal leakage and efficient updates on commodity hardware. In *Selected Areas in Cryptography - SAC 2015 - 22nd International Conference, Sackville, NB, Canada, August 12-14, 2015, Revised Selected Papers*, pages 241–259, 2015.