Geometriai kódok

Csirmaz László[*] Gyula. O. H. Katona[†]

Absztrakt

Az elmúlt évek egyik fontos kutatási területe a kriptográfiai műveleteket végző illetve azok végrehajtását segítő fizikai objektumok vizsgálata. Például bizonyos fizikai objektumok speciális tulajdonságai kihasználva azokkal egyirányú függvényeket lehet számoltatni. A cikkben a lehető legegyszerűbb esetet tekintjük, nevezetesen amikor egy kriptográfiai kulcsot (bitsorozatot) kívánunk előállítani a mérési eredményből. A fizikai objektum ebben az esetben úgy működik mint egy valódi kulcs, azzal az igen hasznos további tulajdonsággal, hogy lehetetlen még egy példányban előállítani. Különböző alkalmakkor mérve persze az eredmények különbözők lesznek, a mérésből előálló bitsorozatnak azonban mindig ugyanannak kell lennie. Egy matematikai modellt állítunk fel és a modell segítségével megvizsgáljuk mik a fontos paraméterek, és paraméterek értékei között milyen összefüggésnek kell fennállnia hogy a megfelelő mennyiségű és minőségű kriptográfiai kulcsot ki tudjuk nyerni.

1 Bevezetés

Különböző fizikai objektumok speciális tulajdonságait ügyesen használva azok segítségével kriptográfiai műveletek tudunk elvégeztetni. Ilyen módszereket alaposan vizsgáltak [4, 9], sőt az egyik eredmény még a Science folyóiratba is bekerült [10]. Mi arra az egyszerű esetre koncentrálunk, amikor egy fizikai objektum – amit kriptográfiai *bélyegnek* is szokás nevezni – azonosításra szolgál, egyediséget, hitelességet garantál. Ilyen bélyeget például egy DVD-re lehet ragasztani úgy, hogy a DVD tartalmát a bélyegből kivonható kulccsal titkosítják. Mivel a bélyeg előállítása fillérekbe kerül, másolása pedig csak hihetetlenül költséges eljárásokkal lehetséges, ha lehetséges egyáltalán, egy ilyen megoldás megoldaná a DVD-k másolásával kapcsolatos gondokat. Papír alapú dokumentumok eredetiségét lehet igazolni a papírra erősített bélyeggel, ha a bélyegből kivonható kulcsot, és a dokumentum tartalmát a kibocsátó például digitálisan aláírja. Bélyeget bankkártyára téve meg lehet akadályozni annak másolását, feltéve ha a kártya csak a bélyegből kivont kulccsal tud dolgozni.

Kriptográfiai bélyeg szinte bármilyen fizikai objektum lehet, amit ismételten meg lehet mérni. Jó néhány szabadalom is létezik. A [1] szabadalom mágneses szálakat használ, amiket egy vékony rétegre fröcsköltek fel. A méréséhez a bélyeget egy közönséges mágnesszalag olvasó előtt kell elhúzni. A [5] szabadalom azt használja ki, hogy amikor egy papírlapot nagy fényerejű lámpa előtt elhúzunk, különböző sötétebb-világosabb foltok jelennek meg. A [6] apró vezető részecskéket használ, amik egy szigetelő rétegbe vannak eloszlatva, és mikrohullámú berendezést használ az információ kiolvasásához. A szabadalmak áttekintése megtalálható [9]-ben, ahol azt a lehetőséget vizsgálják, amikor a bélyeg átlátszó

[*]Közép Európai Egyetem
[†]Rényi Intézet

epoxigyantába ágyazott üveggömbökből áll. Papír alapú tárgyaknál a bélyeg állhat a papírba ágyazott speciális szálakból, a mérés történhet például ultraibolya fényben, amiben ezek a szálak világítanak. És persze a közönséges ujjlenyomat, íriszkép, tenyér- illetve hanglenyomat is tekinthető kriptográfiai bélyegnek.

A mérés eredménye egy sor digitalizált adat, amit egy szkenner vagy egyéb speciális készülék szolgáltat. Az adat különböző szűrőkön, simításon, levágáson megy keresztül, esetleg további ravasz adatfeldolgozási technikákat is használnak. Ez a feldolgozás lényegesen csökkenti az adat mennyiségét, de feltehetően megtartja az objektum fontos fizikai jellemzőit. Végezetül az előfeldolgozott adatból származtatják majd a kriptográfiai kulcsot.

A cikkben ennek a folyamatnak egyetlen részére koncentrálunk, nevezetesen arra, hogyan lehet a kriptográfiai kulcsot kinyerni. Ebből a szempontból az előfeldolgozást tekinthetjük akár a mérés részének, akár a kulcs kinyerésére szolgáló eljárás részének. Magát a fizikai objektumot azonosítjuk egy tökéletes mérés eredményével. Minden más (valódi) mérés a tökéletes méréstől különböző, de hozzá "elegendően közeli" eredményt ad, bármit is jelentsen ez. Várakozásainknak megfelelően ugyanannak az objektumnak mérései ugyanazt a kulcsot kell adják, vagyis elegendően közeli mérések eredményei ugyanazt a kivonatot kell eredményezzék.

Képzeljük el, hogy egy mérés eredménye egy mondjuk egymillió képpontból álló digitalizált szürke kép. Minden pixelben ismerjük az intenzitást, ami egy 0 (fekete) és 1 (fehér) közötti valós szám. Ekkor az egész kép tekinthető az 1 millió dimenziós Euklideszi tér egy vektorának. Két kép "elegendően közel van" egymáshoz, ha mondjuk pixelenként az intenzitások átlagos eltérése kisebb mint 1 százalék. Más szavakkal a vektorok közötti távolságot L_1 normában mérjük, és a még megengedett távolság 0,01-szer 1000000, vagyis 10000. Pixelek helyett a képet áttranszformálhatjuk a frekvenciatartományba. Képek hasonlóságát jobban méri az, hogy mennyire van közel a frekvenciaképük. Mind az apró, mind a nagy méretű, teljes képre kiterjedő szisztematikus hibák könnyen kiszűrhetők, ha a magas illetve alacsony frekvenciájú összetevőket kis súllyal vesszük figyelembe. Diszkrét frekvenciaértékeket választva a képet megint valós számok sorozataként – tehát vektorként – írhatjuk le, és a képek távolsága ebben a térben is valamilyen norma.

Modellünkben feltesszük hogy a mérés valamilyen M *fázistér* egy pontját adja vissza. A mérések "közelségét" egy távolságfüggvény adja meg, tehát M-ben van metrika. A fizikai objektumokat (bélyegeket) az ideális mérés eredményével azonosítjuk, tehát a fizikai objektumokat is M elemeinek tekintjük. Mivel egy bélyeg valamilyen értelemben véletlen objektum, ennek modellezéséhez a fázistérben egy μ mértékre is szükség van: a lehetséges bélyegek egy A részhalmazára $\mu(A)$ adja meg annak a valószínűségét, hogy egy véletlenszerűen választott bélyeg A-ba esik.

Ha ismerjük egy mérés eredményét, vagyis M egy p pontját, akkor valamilyen tovább nem részletezett eljárás megmondja mi a hozzá tartozó kriptográfiai kulcs. Minden egyes k kulcsra legyen A_k azoknak a pontoknak a halmaza, amikhez a k kulcs tartozik. Amikor a $p \in M$ objektumot megmérjük, akkor az eredmény egy $p' \in M$, ami elegendően közel van p-hez, vagyis p és p' távolsága kisebb vagy egyenlő mint valamilyen pozitív ε. A p'-höz tartozó kulcsnak persze ilyenkor ugyanannak kell lennie mint a p-hez tartozó kulcsnak.

Az A_k halmazok egyértelműen meghatározzák, hogyan kell a mérésekhez a kulcsokat hozzárendelni. Egy ilyen rendszer tulajdonságai szoros kapcsolatban vannak az A_k halmazok geometriai tulajdonságaival, ezért az A_k halmazok családját, amint k végigfut a lehetséges kulcsokon, *geometriai kód*nak nevezzük.

A geometriai kódoknak három fontos paramétere van: az *előny*, a *biztonság* és a *hibatűrés*. Az *előny* egy $\alpha \geq 1$ valós szám, azt adja meg, hogy átlagosan hány véletlen bélyeget kell választanunk amíg egy érvényeset találunk, vagyis amíg a választott p pont beleesik valamelyik A_k halmazba. Ha az előny nagy, akkor várhatóan sok bélyeget kell eldobnunk amíg egy használhatót kapunk. Ha az előny közel van 1-hez, akkor majdnem az összes bélyeg használható. Az ideális esetben az előny értéke 1, amikor is mindegyik bélyeg (1 valószínűséggel) jó. A *hibatűrés* azt mondja meg, hogy egy méréskor mekkora hibát véthetünk. Ha ez az értéke ε és $p \in A_k$, akkor p-t megmérve az eredményül kapott p' és p távolsága legfeljebb ε lehet. Mivel p'-ből is ugyanazt a k kódot kell előállítanunk mint p-ből, ez azt jelenti, hogy az A_k halmazok ε sugarú környezetei diszjunktak kell legyenek. Végül a *biztonság* paraméter az A_k halmazok méretét korlátozza. Ez a σ paraméter mondja meg, hogy ha véletlenszerűen választunk egy p érvényes bélyeget, akkor a belőle előállítható k kulcsot legfeljebb σ valószínűséggel kaphatjuk meg.

Nézzük meg, hogy például ujjlenyomatok esetén mi felel meg a modellben található fogalmaknak. Az [8] összefoglaló műben ismertettek szerint az ujjlenyomatról elsőként egy nagyjából 300-szor 300-as szürke skálájú raszterkép készül. Ezt egy kisméretű optikai leolvasóval, vagy közbetlen kapacitásméréssel készíthetik el. A raszterképen elsőként meghatározzák az ujjlenyomatot meghatározó vonalakat, majd ezeket a vonalakat *vékonyítják* amíg csak egy pixel szélesek nem lesznek. Ezután a *finom jellemzőket* keresik meg. Ezek azok a pontok, ahol egy vonal véget ér, vagy ahol egy vonal kettéágazik (Y-pont). Egy ujjlenyomaton ezek száma néhányszor tíz és száz között változik. Minden ilyen jellemzőről a következő információkat tárolják: a pont típusa (végződés vagy elágazás), a pont helye, illetve a vonal iránya. Az így kapott jellemzőket még szűrik (például a túl közeli, hasonló irányú végződéseket törlik), hogy csökkentsék az olvasás és a feldolgozás során elkövetett hibák hatását.

Mondjuk az ujjlenyomat alapján egy legalább 80 bites fix számot szeretnénk előállítani, és ehhez az ujjlenyomat első húsz jellemzőjét használjuk. Az M *fázistér* a húsz jellemző megadásához szükséges adatokat tartalmazza:

$$\left(\{\mathrm{I}, \mathrm{Y}\} \times [0,1]^2 \times [0,\pi)\right)^{20}.$$

Az első tényező a jellemző típusa (végződés vagy elágazás), a következő a pont két koordinátája, az utolsó pedig az irány; mindezt hússzor ismételjük meg. A *mérték* azt mondja meg, hogy egy véletlen ujjlenyomat mekkora valószínűséggel esik az adott részbe. Az egyszerűség kedvéért a teljes téren a szorzat mértéket választjuk. (Ez annak a feltételezésnek felel meg, hogy az egyes jellemzők függetlenek – ami természetesen nem igaz, hiszen az egyes jellemzők nem kerülhetnek túlságosan közel egymáshoz.) Mivel a jellemzőket mindig elhelyezkedésük alapján sorba rakjuk, azért az M térnek csak egy T részét használjuk fel. A mértéket úgy kell normálni, hogy ennek a T-nek éppen 1 legyen a mértéke.

Az egyes tényezőkben mind a hely, mind az irány bármi lehet, azaz ezekre a szokásos Lebesgue mértéket használjuk. A két elemű $\{\mathrm{I}, \mathrm{Y}\}$ halmazon a mértéket annak megfelelően állapítjuk meg, hogy tipikusan egy ujjlenyomaton a jellemzők között hány százalék a végződés, és hány százalék az elágazás.

A *távolság* az fejezi ki, hogy ugyanannak az ujjnak két különböző méréséből származó adat mennyire van közel. Ha valamelyik tényezőben a típus különbözik, akkor a távolság nagyon nagy – mondjuk 1000 –, egyébként mind a hely, mind az irány különbsége kicsi legyen. A teljes távolság az egyes tényezőkben mért távolságok maximuma lehet.

Ha figyelembe akarjuk venni, hogy a kép elfordulhat, akkor az M fázistér helyett vehetjük azt a faktorteret, melyben M két elemét azonosítjuk, ha azok a négyzet egy elforgatásával/eltolásával egymásba vihetők. Mértékként használhatjuk a faktormértéket (ami persze most már nem lesz egyenletes), a távolság pedig lehet az inverz képek távolságának infimuma. Hasonlóan kezelhetjük azt az esetet amikor egy jellemző kimaradása esetén is "közelinek" szeretnénk elfogadni a két mérési eredményt.

A σ *biztonságot* 2^{-80}-ra választjuk. Ezzel biztosítjuk, hogy a generált számok közül mindegyiket legfeljebb ekkora valószínűséggel kapjuk meg (feltéve hogy a mérték nagyjából egyenletes). Az α *előny* reciproka azt mondja meg, hogy az összes lehetséges mérési eredmény közül legfeljebb mekkora mértékű lehet az, amihez nem tartozik eredmény. Ha valakinek az ujjlenyomata ebbe a kivételes halmazba esne, akkor annak nem tud a rendszer kódszámot generálni. Azt reméljük, hogy az fázistér viszonylag kis része áll elő valódi ujjlenyomatból, így $\alpha = 2$ reális választásnak tűnik.

A *hibatűrés* értékét a legnehezebb előre megmondani. Miután definiáltuk a távolságot, több méréssorozat alapján megbecsülhetjük hogy ugyanarról az ujjról kapott jellemzők sorozata mekkora távolságra kerülhet el.

A 2. részben a pontos definíciókat adjuk meg, kimondjuk és bizonyítjuk a fő eredményünket, ami a geometriai kódok három paramétere ad szükséges feltételt. A 3. részben példákat adunk geometriai kódokra, amik megmutatják hogy a tételben szereplő feltétel konstans szorzó erejéig szükséges is bizonyos fontos esetekben. Megvizsgáljuk hogy a fázistér milyen tulajdonságai szükségesek. Végül az utolsó részben összefoglaljuk az eredményeket.

2 A geometriai kód

Az M fázistér egy μ mértékkel ellátott tér, amin még egy $d(x, y)$ távolság is van. A p pont körül ϱ sugarú (nyílt) gömb azoknak az M-beli pontoknak a halmaza, melyek ϱ-nál közelebb vannak p-hez. Ezt a gömböt $p + \varrho$-val fogjuk jelölni:

$$p + \varrho \stackrel{\text{def}}{=} \{x \in M \,:\, d(x, p) < \varrho\}.$$

Az M egy tetszőleges A részhalmazára A-nak *ϱ sugarú környezete* a $p + \varrho$ gömbök uniója, ahol p végigfut A elemein:

$$A + \varrho \stackrel{\text{def}}{=} \bigcup\{p + \varrho \,:\, p \in A\}.$$

Ez nem más, mint az M olyan pontjainak halmaza, amik A valamelyik eleméhez ϱ-nál közelebb vannak. $A + \varrho$ az eredmény, ha A-t ϱ-val *meghízlaljuk*. A háromszögegyenlőtlenség miatt ha $A + \varrho_1$-et meghízlaljuk ϱ_2-vel, akkor az eredmény biztosan benne van $A + (\varrho_1 + \varrho_2)$-ben. Azt mondjuk, hogy a metrika *lapos*, ha ez a tartalmazás pozitív ϱ_1 és ϱ_2 esetén soha sem valódi, vagyis ha minden pozitív ϱ_1 és ϱ_2 mellett

$$(A + \varrho_1) + \varrho_2 = A + (\varrho_1 + \varrho_2). \tag{1}$$

Természetesen fel kell tennünk, hogy minden gömb mérhető a μ mérték szerint. Ennél azonban többet követelünk meg, nevezetesen azt, hogy a mérték *homogén* legyen, vagyis az azonos sugarú gömbök mind ugyanakkor mértékűek. A ϱ sugarú gömb mértékét (vagyis térfogatát) $V(\varrho)$-val fogjuk jelölni. Még azt is feltesszük, hogy ez a V függvény folytonos, szigorúan monoton nő és minden értékkészlete a nem-negatív valós számok halmaza. Ha $A \subseteq M$ egy mérhető halmaz, akkor $r(A)$-val jelöljük annak a gömbnek a sugarát, aminek térfogata megegyezik A mértékével, vagyis

$$\mu(A) = V(r(A)).$$

Ezen kívül rögzítjük a fázistér egy egységnyi mértékű T részét is. A T elemei lesznek a mérések lehetséges kimenetelei. Ha $A \subseteq T$, akkor a $\mu(A)$ mértéket úgy értelmezzük, mint annak a valószínűségét, hogy a mérés eredménye A-ba esik.

Például M lehet az $\mathbb{R}^n$-nek jelölt n dimenziós Euklideszi tér a szokásos távolsággal, T a térben az egységkocka, μ pedig a Lebesgue mérték. Ez a mérték annak felel meg, amikor a fázis tér pontjait egyenletes eloszlással választjuk ki.

1. Definíció Egy m méretű *geometriai kód* a T-nek m darab mérhető részéből álló $\{A_k \,:\, 1 \leq k \leq m\}$ sorozat. A kód *biztonsága* σ, ha minden k-ra $\mu(A_k) \le \sigma$;

előnye α, ha $\mu(\bigcup A_k) \ge 1/\alpha$; és

hibatűrése ε, ha A_k-nak az ε-környezete még mindig része T-nek és ezek az ε-környezetek páronként diszjunktak, vagyis $A_k + \varepsilon \subseteq T$, valamint $(A_i + \varepsilon) \cap (A_j + \varepsilon) = \emptyset$ ha i és j különbözőek.

A *biztonság* azt garantálja, hogy mindegyik kulcsot legfeljebb σ valószínűséggel kaphatjuk meg, feltéve hogy a bélyeget véletlenszerűen választjuk. A paraméter értékét 2^{-50} vagy annál kisebbre kell választani. Az *előny* az az érték, ahány bélyeget várhatóan generálnunk kell ahhoz, amíg egy használhatót (vagyis valamelyik A_k-ba esőt) kapunk. Ennek tipikus értéke $1,5$ és 100 között kell legyen. Végül a *hibatűrés* azt mondja meg, hogy mekkora hibát követhetünk el a méréskor: ha egy bélyeg mondjuk A_k-ba esik, és megmérjük, akkor a mérési eredmény A_k-nak ε sugarú környezetébe esik. Azt akarjuk, hogy ebből a mérésből egyértelműen megállapíthassuk a bélyeghez tartozó kulcsot. Ezért ezeknek a környezeteknek diszjunktaknak kell lenniük.

A modellünkből azonnal adódik, hogy egy geometriai kód előnye csak akkor lehet 1, ha hibatűrése 0. Ha a mérés eredményeképpen bármiféle hibát megengedünk, akkor kell lennie T-ben olyan pontnak, amihez nem tartozik kulcs. Ez különösen problematikus, ha T valamilyen biometriai mérték – például ujjlenyomat, vagy íriszkép –, hiszen nem lehet valaki a rendszerből kizárni azért, mert "nem elég jó az ujjlenyomata."

Mivel a mérési eredményekhez a kriptográfiai kulcsokat az A_k halmazok segítségével rendeljük hozzá, az A_k halmazoktól még további tulajdonságokat is megkövetelhetünk. Például hogy az összes A_k ugyanakkor, vagy majdnem ugyanakkora valószínűségű legyen, ami azt jelenti hogy a generált kulcsot nagyjából egyenletesen eloszlásban kapjuk meg. Azután az sem árt, ha az A_k halmazok elég "egyszerűek," vagyis a mérési eredményből a kulcs előállítása ne legyen túlságosan nehéz.

A geometriai kódok definiáló tulajdonságai természetesen adódnak a modellezendő feladatból. Az egyetlen kivétel talán az a megszorítás, hogy az A_k halmazok ε környezete még mindig része legyen T-nek. Ez az egyszerűsítő feltétel áttekinthetőbbé teszi az eredményeinket és a bizonyítást is. Bizonyos esetekben lényeges különbséget jelenthet ez a megszorítás, erre is fogunk látni példát.

2. Definíció Az M fázistér *Brunn-Minkowski tulajdonságú*, ha minden mérhető A halmazra

$$\mu(A + \varepsilon) \ge \mu\big((p + r(A)) + \varepsilon\big).$$

Más szavakkal egy A halmaz akkor hízik a legkevesebbet, ha az egy gömb. A bal oldalon az A halmazt hízlaltuk meg ε-nal, jobboldalon pedig az A-val megegyező térfogatú gömböt. Ha a metrika lapos, akkor az egyenlőtlenség a következő egyszerűbb alakba írható:

$$r(A + \varepsilon) \ge r(A) + \varepsilon.$$

A nevezetes *Brunn-Minkowski egyenlőtlenség* azt mondja ki, hogy az n-dimenziós Euklideszi tér a szokásos távolsággal és a Lebesgue metrikával Brunn-Minkowski tulajdonságú [2]. A tételnek számos általánosítása van például hiperbolikus terekre is.

Minden definíció a rendelkezésünkre áll, hogy kimondjuk és bizonyítsuk a fő tételt, természetesen nem a lehető legáltalánosabb formában.

1. Tétel *Tegyük fel, hogy az M fázistér lapos, Brunn-Minkowski tulajdonságú, és a ϱ sugarú gömb térfogatát megadó $V(\varrho)$ függvény log-konkáv. Ekkor egy geometriai kód α, σ, ε paraméterei kielégítik az alábbi egyenlőtlenséget:*

$$\varepsilon \leq V^{-1}(\alpha\sigma) - V^{-1}(\sigma). \tag{2}$$

Bizonyítás Tegyük fel, hogy a geometriai kód az $A_1, \ldots, A_m$ halmazokból áll. Legyen $r(A_k) = a_k$, vagyis a_k annak a gömbnek a sugara, aminek ugyanakkor a térfogata mint A_k-nak. Mivel M lapos, azért a Brunn-Minkowski egyenlőtlenség második alakját alkalmazhatjuk, ami szerint $r(A_k+\varepsilon) \geq r(A_k)+\varepsilon = a_k + \varepsilon$. Más szavakkal, $A_k + \varepsilon$ legalább akkora térfogatú mint az $a_k + \varepsilon$ sugarú gömb:

$$\mu(A_k + \varepsilon) \geq V(a_k + \varepsilon). \tag{3}$$

Legyen még a annak a gömbnek a sugara, aminek térfogata éppen σ, vagyis $a = V^{-1}(\sigma)$. Mivel a kód biztonsága σ, ez azt jelenti hogy $\mu(A_k) \leq \sigma$, ahonnan $a_k \leq a$ minden k-ra.

Mind $a_k+\varepsilon$, mint a eleme az $(a_k, a+\varepsilon)$ intervallumnak, továbbá ha $a_k+\varepsilon$ az intervallumot $\lambda : 1-\lambda$ arányban osztja, akkor a ugyanezt az intervallumot $1-\lambda : \lambda$ arányban osztja. Feltételünk szerint a $\log V$ függvény konkáv, tehát

$$\begin{aligned} \log V(a_k+\varepsilon) &\geq (1-\lambda)\log V(a_k) + \lambda \log V(a+\varepsilon), \\ \log V(a) &\geq \lambda \log V(a_k) + (1-\lambda)\log V(a+\varepsilon). \end{aligned}$$

Ezeket összeadva és átalakítva kapjuk, hogy

$$V(a_k+\varepsilon) \geq \frac{V(a+\varepsilon)}{V(a)} \cdot V(a_k).$$

A (3) szerint a bal oldal értéke legfeljebb $\mu(A_k + \varepsilon)$. Az $A_k + \varepsilon$ halmazok a T diszjunkt részei, tehát mértékük összege nem haladhatja meg T mértékét, ami 1:

$$1 = \mu(T) \geq \sum_k \frac{V(a+\varepsilon)}{V(a)} \cdot V(a_k) = \frac{V(a+\varepsilon)}{V(a)} \sum_k V(a_k) \geq \frac{V(a+\varepsilon)}{V(a)} \cdot \frac{1}{\alpha},$$

itt kihasználtuk hogy $V(a_k)$ az A_k halmaz mértéke, ezért $\sum_k V(a_k) = \mu(\bigcup A_k) \geq 1/\alpha$. Ha még felhasználjuk, hogy $V(a) = \sigma$, éppen (2)-t kapjuk. ■

3 Példák

Első példánkban M az n dimenziós Euklideszi tér a szokásos távolsággal és a Lebesgue mértékkel. A kódok lehetséges T halmaza lehet például az egységkocka, vagy az 1 térfogatú gömb. A ϱ sugarú n-dimenziós gömb térfogata

$$V(\varrho) = \gamma_n \varrho^n \qquad \text{ahol} \qquad \gamma_n = \frac{\pi^{n/2}}{(n/2)!}.$$

Világos, hogy $V(\varrho)$ log-konkáv (hiszen $\log V(\varrho)$ lineáris függvény), és hogy $\mathbb{R}^n$ Brunn-Minkowski tulajdonságú (lásd [2]). A $k!$ értékét $(k/e)^k$-nal közelítve az 1. tétel egyenlőtlensége a következőképpen alakul:

$$\varepsilon \leq \sqrt{\frac{2\pi e}{n}}\, \sigma^{1/n} \left(\alpha^{1/n} - 1\right). \tag{4}$$

Ha n legalább tízszer akkora, mint $\log\alpha$, akkor a jobb oldal utolsó tényezője helyettesíthető a $(\log\alpha)/n$ kifejezéssel. Ha most α-t és σ-t fixen tartjuk, akkor a jobb oldal a legnagyobb értékét az $n \approx 0,66$ $\log(1/\sigma)$ helyen veszi fel, függetlenül α értékétől. Ezt (4)-be helyettesítve kapjuk, hogy

$$\varepsilon \leq \frac{2}{3}e^{2/3}\sqrt{2\pi e}\,\frac{\log\alpha}{\log(1/\sigma)} \approx 5,37\,\frac{\log\alpha}{\log(1/\sigma)}.$$

Ha például $\sigma = 2^{-50}$ és $\alpha = 1,5$, akkor az innen adódó korlát $\varepsilon \leq 0,01$, és n értékét 23 körül kell megválasztani.

Ebben a fázistérben tudunk olyan geometriai kódokat konstruálni, melyek a (4) korlátot jól megközelítik. A konstrukció a következőképpen működik. Vágjunk ki diszjunkt $\sigma^{1/n} + 2\varepsilon$ élhosszúságú kockákat T-ből, és mindegyik kis kockát zsugorítsuk össze a középpontjából annyira, hogy az élhossza $\sigma^{1/n}$ legyen. Az így kapott zsugorított kockák egy geometriai kódot alkotnak, melynek biztonsága σ (hiszen mindegyik ilyen kis kocka térfogata éppen σ), és hibatűrése ε. A kód előnye attól függ, hogy hány kis kockát tudunk T-ből kivágni. Az egyszerűbb számítás érdekében tegyük fel hogy T az egységkocka. Mivel a kis kockák élhossza $\sigma^{1/n} + 2\varepsilon$, T-ből legalább

$$\left[\frac{1}{\sigma^{1/n}+2\varepsilon}\right]^n \geq \left(\frac{1}{\sigma^{1/n}+2\varepsilon} - 1\right)^n$$

ilyen kockát tudunk kivágni. A kód előnye α, ha

$$\left(\frac{1}{\sigma^{1/n}+2\varepsilon} - 1\right)^n \sigma \geq \frac{1}{\alpha},$$

ami fennáll hogyha

$$\varepsilon \leq 0,5\,\sigma^{1/n}\left(\alpha^{1/n}\,\frac{1}{1+(\alpha\sigma)^{1/n}} - 1\right). \tag{5}$$

Ha $(\alpha\sigma)^{1/n}$ elegendően kicsi, akkor ez a (4)-ból adódó elméleti korlát $10\sqrt{n}$-szerese.

Általában ha ∂T jelöli a T felszínét, akkor T-ből legalább

$$\frac{1-\eta\sqrt{n}\,\partial T}{\eta^n}$$

darab η élű kockát tudunk kivágni. Ha még feltesszük, hogy $x = \eta\sqrt{n}\,\partial T$ kisebb félnél, akkor $(1-x)^{1/n}$-t közelíthetjük $1 - x/n$-nel, ami mutatja, hogy tudunk létezik α előnnyel geometriai kód ha

$$\varepsilon \leq 0,5\,\sigma^{1/n}\left(\alpha^{1/n}\,\frac{1}{1+\dfrac{\partial T}{\sqrt{n}}(\alpha\sigma)^{1/n}} - 1\right). \tag{6}$$

A konstansszor $(\alpha\sigma)^{1/n}$ hibatag a *kerületi hiba*, ez abból adódik, hogy a T határához közeli pontokat nem tudjuk felhasználni. Ez az érték arányos T felszínével, és nullához tart ha σ tart nullához. Az itt álló $0,5$ konstans és a (4)-beli $\sqrt{2\pi e/n}$ konstans közti eltérés a *pakolási hiba*. Ez abból adódik, hogy az n-dimenziós gömböket nem lehet szorosan pakolni.

Ha T éppen az egység térfogatú gömb, akkor a kerületi hiba $1+\sqrt{2\pi e}\,(\alpha\sigma)^{1/n}$. Ez például (6)-ből vagy közvetlenül is kiszámolható.

A Lebesgue mérték megtartásával más távolságfüggvényt is használhatunk $\mathbb{R}^n$-ben. A távolságot legegyszerűbben egy *norma* segítségével definiálhatunk: az x és y pontok (mint vektorok) távolsága az $x-y$ különbség normája:

$$d(x,y) \stackrel{\text{def}}{=} ||x-y||.$$

Az így definiált metrikus tér mindig lapos, és a "gömbök" konvex halmazok. Következésképp ezekben a fázisterekben szintén teljesül a Brunn-Minkowski tulajdonság, lásd [2]. A ϱ sugarú "gömb" térfogata $V(\varrho)=c\cdot\varrho^n$, ahol c a $B_1=\{x\in\mathbb{R}^n : ||x||<1\}$ egységgömb térfogata. Mivel a $V(\varrho)$ függvény most is log-konkáv, alkalmazhatjuk az 1. tételt, ami a következő elméleti korlátot adja:

$$\varepsilon \le \frac{1}{c^{1/n}}\,\sigma^{1/n}\left(\alpha^{1/n}-1\right). \tag{7}$$

Ha a maximum, vagyis L^∞-normát használjuk, akkor a "gömbök" éppen az n-dimenziós kockák lesznek. Az egység sugarú gömb ebben az esetben a kettő élhosszúságú kocka, tehát $c=2^n$. A (7) korlátban a konstans értéke éppen $0,5$. Mivel kockákkal a tér hézag nélkül kitölthető, azt várjuk hogy létezzen olyan geometriai kód, melyben nincs pakolási hiba. A számítások mutatják, hogy ténylegesen is ez a helyzet: a (5) határ ugyanazzal a konstrukcióval most is elérhető.

Általában tetszőleges normából származó távolságfüggvény esetén is léteznek az elméleti (7) korlátot elég jól megközelítő konstrukciók. A B_1 "egységgömb" ebben az esetben szükségszerűen konvex. Mint minden konvex test, B_1 is befoglalható egy olyan téglatestbe, melynek térfogata legfeljebb $n!$-szorosa B_1 térfogatának. Legyen φ az az affin transzformáció, ami ugyanakkor térfogatú kockát csinál ebből a téglatestből. Ez a transzformáció a T alakzatot φT-be viszi. A T belsejében csupa kis téglalapból álló (α, σ, ε) paraméterű geometriai kódot tudunk konstruálni ha

$$\varepsilon \le \frac{1}{(n!)^{1/n}c^{1/n}}\,\sigma^{1/n}\left(\alpha^{1/n}\frac{1}{1+\dfrac{\partial\varphi T}{\sqrt{n}}(\alpha\sigma)^{1/n}}-1\right).$$

A kerületi hibától eltekintve a két korlát az $(n!)^{1/n}\approx n/e$ konstans erejéig megegyezik.

Láttunk példákat, ahol a fázistér pontjai az n-dimenziós Euklideszi tér vektorai voltak, és a távolságot tetszőleges normából definiáltuk. Ezek a terek rendelkeznek néhány természetes, elvárható tulajdonsággal; ezek közül négyet külön fölsorolunk:

(i) a távolság eltolásinvariáns, vagyis a és b között ugyanaz a távolság, mint $a+x$ és $b+x$ között minden x vektorra;

(ii) a tér lapos;

(iii) a távolság a szokásos Euklideszi topológiát generálja;

(iv) a mérték homogén, vagyis egyenlő sugarú gömbök ugyanolyan mértékűek.

További eredményünk, hogy az 1. tétel állítása igaz az összes, az n-dimenziós Euklideszi tér pontjain definiált fázistérben, melyek ezekkel a tulajdonságokkal rendelkeznek.

2. Tétel *Tegyük fel, hogy az M fázistér az n-dimenziós Euklideszi tér pontjain van definiálva, és teljesíti a fenti* (i)–(iv) *tulajdonságokat. Ekkor ebben a térben minden geometriai kód paraméterei teljesítik az 1. Tételben felírt feltételt.*

A tétel bizonyításához elegendő megmutatni, hogy az (i)–(iv) feltételek biztosítják, hogy a mérték csak a Lebesgue-mérték lehet, a távolság pedig valamilyen normából származik. Ezekre a fázisterekre az 1. Tétel közvetlenül alkalmazható.

Tudunk példát mutatni arra, hogy a (ii) feltétel szükséges. Ebben a teret a kétdimenziós Euklideszi tér pontjain definiáljuk. A mérték a szokásos, a távolságot viszont speciálisan kellett megválasztani. Ez a tér nem lehet Brunn-Minkowski tulajdonságú.

4 Összefoglalás

A cikkben egy gyakorlati feladat során felmerült probléma absztrakt matematikai modelljét adtuk meg. A feladat az volt, hogy véletlen tulajdonságokkal rendelkező fizikai objektumhoz rendeljünk fix kriptográfiai kulcsot, melyet az objektum megmérésével elő tudunk állítani. A modellnek három fontos paraméter volt: a *biztonság*, az *előny* és a *hibatűrés*. Igazoltunk e három paraméter között fennálló egyenlőtlenséget, ami a geometriai kód mögött található fázistér geometriai tulajdonságaiból következett.

Részletesen megvizsgáltuk azt az esetet, amikor a fázistér az n-dimenziós Euklideszi tér a szokásos Lebesgue mértékkel, de nem feltétlenül a szokásos L^2 távolsággal. Konstrukciókat adtunk meg, amik az elméleti korlátot bizonyos hibákkal érték el. Két típusú hibatagot azonosítottunk. A *kerületi hiba* abból adódik, hogy a geometriai kód nem tudja kihasználni a fázistér megengedett részének a határát. A *pakolási hiba* pedig azt méri, mennyire sűrűn lehet a teret "gömbökkel" kitölteni.

A konstrukcióknak még további szép tulajdonságai is voltak. Mindegyik kódban a halmazok ugyanakkora térfogatúak voltak, és mindegyik vagy kocka vagy téglatest volt. Az egyszerű struktúra miatt a kulcs kiszámítása hatékonyan történhet.

Megvizsgáltuk azokat a feltételeket, melyeket a fázistérről tettünk. Az egyik a nevezetes Brunn-Minkowski egyenlőtlenség általánosítása; egy másik egy különös feltétel a távolságfüggvényre, nevezetesen hogy a térnek laposnak kell lennie. Igazoltuk, hogy ez utóbbi tulajdonságnak több érdekes következménye van. Az egyik, hogy az r sugarú gömb térfogata legfeljebb exponenciálisan nőhet. Egy másik hogy az n-dimenziós Euklideszi téren definiált fázistereken a metrika lapossága bizonyos további homogenitási tulajdonságokkal együtt már biztosítja hogy a geometriai kódokra vonatkozó (2) egyenlőtlenség fennálljon. Példát konstruáltunk olyan kellemes tulajdonságokkal rendelkező fázistérre, amelyik nem lapos, tehát ez egy nem triviális tulajdonság.

A kettő és többdimenziós hiperbolikus terek szintén teljesítik az 1. tétel feltételeit. Érdekes volna különböző konstrukciókat látni, hogy azok mennyire közelítik meg a (2) alatti elméleti határt. A hiperbolikus térben T határa összemérhető T területével, ezért jelentős különbségekre számítunk ha előírjuk hogy az A_i-k ε sugarú környezete része legyen T-nek, illetve ha ezt nem követeljük meg.

Nagyon sok tér rendelkezik a Brunn-Minkowski tulajdonsággal. Érdekes kérdés, hogy ez a tulajdonság megőrződik-e a szorzatra. Könnyű látni, hogy a valós számegyenes és mondjuk egy kétdimenziós hiperbolikus tér szorzata a maximum normával és a szokásos szorzat metrikával ellátva már nem Brunn-Minkowski tulajdonságú. Sikerült azt is bizonyítanunk, hogy sima M-beli térfogatfüggvény esetén az $\mathbb{R} \times M$ szorzat pontosan akkor Brunn-Minkowski tulajdonságú, ha az M-beli $V(r)$ hatványfüggvény.

Egy másik természetes módon adódó modellben az objektum n különböző jellemzőjét mérjük meg. Ezeknek a mennyiségeknek az értékei alkotják azt az n dimenziós x vektort, amivel magát az objektumot azonosítjuk. A mérésnél minden egyes koordináta a valódi értéktől egy s szórású 0 várható értékű normális eloszlású hibával tér el, a hiba az egyes koordinátáknál független. Ha x' a méréskor kapott vektor, akkor az $x - x'$ különbség L^2 normája szintén egy s szórású, nulla várható értékű normális eloszlású változó. Ha tehát azt akarjuk elérni, hogy az x' mérésből a k kulcsot p valószínűséggel egyértelműen azonosítani tudjuk, ennek feltétele pontosan az, hogy az A_k halmazok ε sugarú környezetei diszjunktak legyenek, ahol ε olyan, hogy egy s szórású. nulla várható értékű normális eloszlású véletlen változó $-\varepsilon$ és ε közé eső értéket éppen p valószínűséggel vegyen fel.

Vizsgálatainkban mindig arra az esetre koncentráltunk, amikor az kód biztonsága nullához tartott. Egészen más típusú, véges bináris kódokat használó konstrukciókra van szükség, ha $\log(1/\sigma)$ kisebb a tér dimenziójánál. Ha a tér dimenzióját növeljük, akkor a felszíntől legalább ε távolságra lévő pontok mértéke exponenciálisan tart a nullához, tehát egy idő után már nem létezhet rögzített σ biztonságú kód. Ha nem követeljük meg, hogy a kódhalmazok ε sugarú környezete is része legyen T-nek (csak azt, hogy páronként diszjunktak legyenek), akkor akármilyen nagy dimenzióban létezik ε hibatűrésű és σ biztonságú kód – feltéve persze hogy ilyen kód egyáltalán létezik. Az intuíció azt sugallja, hogy a dimenzió növelésével egyre "sűrűbb" ilyen kódot tudunk gyártani, vagyis a kódok α előnye tart az 1-hez. Meglepő módon azt sejtjük, hogy ez nem így van, nevezetesen $2^{-n} \leq \sigma$) esetén n dimenzióban a legkisebb előnnyel rendelkező kódok a teljes tér egy legfeljebb $\log_2(1/\sigma)$ dimenziós alterében vannak. Így például ha 50 bites kriptográfiai kulcsra van szükségünk, vagyis $\sigma = 2^{-50}$, akkor nem érdemes 50-nél több független paraméterét megmérni az objektumnak.

További érdekes kérdés ha a folytonos terek helyett diszkrét tereket tekintünk. A [3] cikkben az n hosszúságú 0–1 sorozatok terén néztek több különböző távolságfüggvényt. Az alkalmazott modellben nem egy, hanem egyszerre 2^k különböző geometriai kódot konstruáltak egyszerre úgy, hogy a tér minden pontja valamelyik kódban benne legyen. Ezzel a módszerrel egyrészt elérték, hogy ne legyenek "selejtek," vagyis olyan elemei a fázistérnek, melyek egyik kódban sincsenek benne, másrészt olyan kódokat kellett konstruálni, melyben az előny 1-hez közeli érték helyett 2^k körüli kellett legyen. Hasonló konstrukciók a folytonos esetben is vizsgálhatók.

Irodalom

[1] J. Brosow: Method and system for verifying authenticity safe against forgery, US patent no 4218674, 1980

[2] Yu. D. Burago, V. A. Zalgaller: *Geometric Inequalities*, Springer, 1988

[3] Y. Dodis, L. Reyzin, A. Smith, *Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data*, Lecture Notes in Computer Science, Vol 3027, pp 523–540, Springer, 2004

[4] B. Gassend, D. Clarke, M. van Dijk, S. Devadas, *Controlled Physical Unknown Functions*, MIT LCS TR-845, 2002

[5] R. Goldman: Verification system for document substance and content, US patent no 4568936, 1986

[6] G. Lippner, personal communication, 2002

[7] A. J. Menezes, P. C. van Oorshot, S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press 1996

[8] L. O'Gorman, *Overview of fingerprint verification technologies*, Elsevier Information Security Technical Report, Vol 3, No 1, 1998

[9] Ravi Pappu, *Physical one-Way Functions*, PhD Thesis, March 2001

[10] Ravi Pappu, Ben Recht, Jason Taylor, Neil Gershenfeld, *Physical One-Way Functions*, Science 2002 September 20, 297, pp 2026–2030

[11] J. Samyn, Method and apparatus for checking the authenticity of documents, US patent no 4820912, 1989