SZEGEDI TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI ÉS INFORMATIKAI KAR
MŰSZAKI INFORMATIKA TANSZÉK
Informatika Doktori Iskola

Véletlenszerű fluktuációk analízisén és hasznosításán alapuló mérési és titkosítási eljárások vizsgálata

Doktori értekezés tézisei

Készítette:
Vadai Gergely

Témavezető:
Dr. Gingl Zoltán
tanszékvezető egyetemi tanár

SZEGED
2018

1 Bevezetés

A természettudományok elmúlt évszázadban történt paradigmaváltásai a természettörvények általános jellegéről alkotott képünkre is hatással voltak. Míg hagyományosan a jelenségek megjósolhatatlanságának okaként a rendszerek bonyolultságára és a determinisztikus összefüggéseket leíró egyenletek ismeretlen kezdőfeltételeire tekintettek, a kvantumfizika rávilágított, hogy bizonyos folyamatok csak a véletlenszerűség felhasználásával írhatóak le megfelelően.

A véletlenszerű jelek – továbbiakban „zajok" – így nem szükségszerűen hátráltató, kiküszöbölendő tényezők, hiszen információt is hordozhatnak a vizsgált rendszerekről, elég az autó motorjának vagy a forrásban lévő víz akusztikus zajára gondolni. Műszaki területeken az áramköri komponensek esetén a zajspektrum azok megbízhatóságáról árulkodik, szívritmusunk ingadozása pedig az egészségi állapotunkról szolgáltat hasznos információt.

Ezen túlmenően a zajok konstruktív szerepet is kaphatnak; egyes rendszerek optimális működését éppen a zajok megfelelő alkalmazása teheti lehetővé, melyre jó példa a mikroelektronika, képfeldolgozás és távközlés területén is elterjedt dithering módszere vagy a tudományos berkekben nagy figyelmet kapott sztochasztikus rezonancia. Az ilyen irányú vizsgálatok és alkalmazások számos tudományág különböző területein is igen hasznosnak bizonyultak.

Doktori tanulmányaim során a Zaj és nemlinearitás kutatócsoport tagjaként lehetőségem adódott számos különböző, multidiszciplináris kutatásba bekapcsolódni. Értekezésemben ezek közül a zajok információforrásként illetve konstruktív szerepben való felhasználásának egy-egy példájául szolgáló alkalmazási területen elért eredményeimet mutatom be. Az ezeket összegző tézispontokat a 4. fejezetben található 1. táblázatnak megfelelően az [1-6] publikációk támasztják alá, míg a [7-9] publikációim ezekhez közvetve kapcsolódnak.

A zajkutatás területén mind a folyamatok analitikus leírása és modellezése, mind a kísérleti vizsgálatok, mérési eredmények statisztikai elemzéséből levont következtetések igen nagy szerepet játszanak. Jól mutatják ezt az értekezés fő eredményei is: a zaj alapú titkosítási protokollok abszolút biztonságosságának elméleti bizonyítását és általánosítását matematikai módszerekkel, a statisztika és valószínűségelmélet eszköztárával végeztem, míg a kajakos sportolók mozgásjeleinek fluktuációiban mutatkozó trendek kimutatása a jelek megfelelő mérését, feldolgozását, időbeli és spektrális analízisét, majd a mérőszámok statisztikai kiértékelését igényelte. Az így tett megállapításaim így sokkal inkább a fluktuációanalízis újszerű területen való hasznosságára és a bevezetett, jel-zaj viszonyon alapuló módszer hatékonyságára világítanak rá.

2 Zaj alapú abszolút biztonságos kommunikáció

A napjainkban használatos kriptográfiai eljárások biztonságossága azon alapszik, hogy a lehallgató (Eve) nem rendelkezik elegendő erőforrással ahhoz, hogy a ma ismert módszerekkel gyakorlati szempontból elfogadható időn belül feltörje azt. Ezt feltételes biztonságnak (conditional security) nevezzük, és természetesen a technológia fejlődéséből adódóan a ma ide sorolt eljárások idővel feltörhetővé válhatnak, ahogyan számos korábban elterjedt módszer esetén történt.

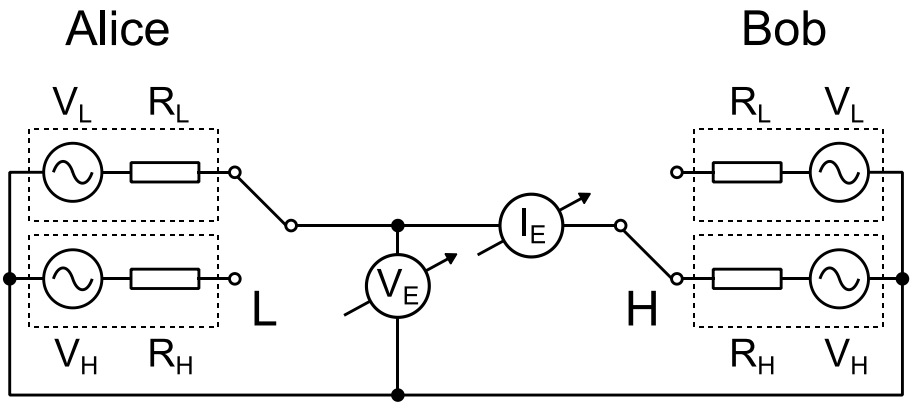
Információelméleti szempontból akkor nevezünk egy titkosítási eljárást abszolút biztonságosnak (unconditonally secure), ha Eve akkor sem jut semmilyen információhoz a nyílt szöveggel kapcsolatban (a hosszán kívül), ha számára végtelen számítási kapacitás és idő áll rendelkezésre. Ez abban az esetben lehetséges, ha a titkosítás alapját képező, kritikus információt jelentő kulcsot csak egyszer használjuk, az teljesen véletlenszerű, és hossza legalább akkora, mint a titkosítandó adaté [10]. Ezt nevezzük egyszer használatos bitmintának (One-Time Pad, OTP).

A kulcsot ehhez azonban mindkét kommunikáló félnek előzetesen ismernie kell, vagy biztonságosan ki kell cserélniük egymással, amely gyakran az eredeti titkosítási feladathoz vezet vissza. Erre a problémára nyújtanak megoldást a kulcsmegosztó (vagy más néven kulcsgeneráló) módszerek, melyek célja nem egy előre elkészített kulcsbitsorozat biztonságos eljuttatása a másik félnek, hanem egy fizikai mennyiség mérésével a kulcsbiteknek a kommunikáció során való közös generálása úgy, hogy Eve ne tudja azt meghatározni anélkül, hogy fel ne fedje a lehallgatás tényét. Ilyen módszer a kvantumos kulcsmegosztás (Quantum Key Distribution, QKD) [11], illetve a következőkben vizsgált, Kish László Béla által 2005-ben bevezetett zaj alapú titkosítás, a Kirchhoff-Law-Johnson-Noise (KLJN) kulcsmegosztó protokoll [12].

A KLJN kulcsmegosztó protokoll

A KLJN protokoll az ellenállások termikus zaját felhasználva elegáns és meglepően egyszerű módon nyújt lehetőséget az abszolút biztonságos kommunikáció megvalósítására, ezen felül biztonságossága pusztán a klasszikus fizika törvényein alapszik [12]. A csupán néhány elektronikai alkatrészből álló rendszer egyszerű, nagyságrendekkel kisebb költséggel megvalósítható és robosztus, így ígéretes alternatívát nyújt a kvantumkriptográfiával szemben.

Az 1. ábrán látható KLJN rendszerben a két kommunikáló fél, Alice és Bob azonos értékű ellenálláspárral rendelkezik (R_L, R_H, $R_L \neq R_H$), a kommunikáció során pedig véletlenszerűen kapcsolja annak egyik elemét a kommunikációs vezetékre, amelyen Eve-nek az ellenállások termikus zajából adódó feszültséget ($V_E(t)$) és áramerősséget ($I_E(t)$) van lehetősége mérni. A rendszer négy lehetséges állapotát Alice és Bob kapcsolóit sorrendben tekintve a következőképp jelöljük: LL, LH, HL és HH.



1. ábra: A KLJN rendszer modellje zajgenerátorok alkalmazásával (LH állapotban).

Az ellenállások – az ábrán feszültséggenerátorral reprezentált – termikus zajából következően a vezetéken mérhető áram- és feszültségzaj középértéke nulla, azaz $<I_E(t)>=0$ és $<V_E(t)>=0$, a Kirchhoff-törvények alapján kiszámítható teljesítménysűrűség-spektrumuk és az azokkal arányos varianciájuk pedig termikus egyensúly esetén LH és HL esetben megegyeznek. Mivel a várható érték és szórás a normális eloszlás esetén tökéletesen meghatározzák a mérhető áram- és feszültségzajokat, Eve a két esetet nem tudja statisztikailag megkülönböztetni, azaz nem rendelkezik információval arról, hogy melyik oldalon választották a kis, és melyik oldalon a nagy értékű ellenállást. Ezzel szemben Alice és Bob, ismerve saját kapcsolójának állását, meg tudja mondani a másik fél választását, azaz az LH és HL állapotok esetén egy bitnyi információ biztonságosan megosztható.

A rendszer abszolút biztonságosságának klasszikus fizikai bizonyítása azon alapszik, hogy termikus egyensúlyban a termodinamika 2. főtétele alapján nincs energiaáramlás a két oldal között, azaz nem nyerhető információ a rendszer állapotáról. Mivel nincsen energiaáramlás, a vezetéken mérhető $P=<V_E(t)I_E(t)>$ teljesítmény, azaz $I_E(t)$ és $V_E(t)$ korrelációja nulla [12, 13].

Szobahőmérsékleten a mérhető feszültség- és áramerősség jelek effektív értéke rendkívül kis értékű, azonban külső zajgenerátorok alkalmazásával az 1. ábrán látható módon elérhető a megfelelő jelerősség, mely rendkívül nagy (10^9 K) „virtuális” hőmérsékletnek fel meg. Az elrendezés biztonságosságához ezen ekvivalens hőmérséklet biztosítása szükséges mindkét oldalon, melyhez a független zajgenerátorok által előállított, L és H állapothoz tartozó feszültségzajok varianciájának az ezen állapotokhoz tartozó ellenállások arányával kell skálázódnia.

A kulcscsere során Alice és Bob minden bit esetén véletlenszerűen választ ellenállást, majd a kulcsból a HH és LL állapotokhoz tartozó bitek, azaz az esetek fele törlésre kerül. Alice és Bob egy publikus, autentikált csatornán egyeztetheti a törlendő bitek sorszámát és a vezetéken végzett méréseinek eredményét az aktív támadások elkerüléséhez, majd a kulcscsere végeztével azon az OTP módszerrel rejtjelezett információt is megoszthatják egymással. A Kerckhoff-elvnek megfelelően Eve a rendszerről minden információval rendelkezhet, így ismerheti az

ellenálláspárok értékét és a zajgenerátorok effektív értékét is, a módszer abszolút biztonságosságát az garantálja, hogy az LH és HL eseteket nem tudja megkülönböztetni.

Az ideális KLJN kulcsmegosztó rendszer – stacionárius esetben – abszolút biztonságos, azonban számos támadási kísérlet a gyakorlatban megvalósítható rendszer ideálistól való eltérését használta ki. A kommunikációs vezeték nem nulla értékű ellenállása, a kommunikátorok közötti hőmérsékletkülönbség, az alkatrészek értékének pontatlansága információszivárgást okoz, azaz Eve 50%-nál (a bitek értékének véletlen megtippelésénél) valamivel nagyobb valószínűséggel határozza meg helyesen a kulcsbit értékét. A KLJN rendszer biztonságosságát és bizonyos támadásokkal szembeni kedvező tulajdonságait annak Szegeden történő első hardveres megvalósítása is alátámasztotta [14], illetve az újabb kulcsmegosztó módszerek és további protokollok bevezetését inspirálta. A rendszer egyszerűsége és flexibilitása miatt számos különböző területen is alkalmazható.

Az abszolút biztonságosság zajra vonatkozó feltételei

Gingl Zoltán és Mingesz Róbert pusztán a matematikai statisztika eszközeivel, a korábbiaktól eltérő megközelítésben nem a termikus zajokon alapuló rendszer biztonságosságát vizsgálták, hanem arra keresték a választ, hogy az abszolút biztonságosság milyen, a mesterséges zajgenerátorokhoz tartozó zajparaméterek mellett áll fent [15]. Eredményeik alapján a biztonságosság *szükséges* feltétele, hogy a zajok eloszlása stabilis legyen, – mely eloszlásfüggvények közül csak a normális eloszlás varianciája véges – továbbá a zajok varianciájának teljesítenie kell a következő összefüggést:

$$\frac{\left\langle V_{\mathrm{H}}^2(t)\right\rangle}{\left\langle V_{\mathrm{L}}^2(t)\right\rangle}=\frac{R_{\mathrm{H}}}{R_{\mathrm{L}}}. \qquad (1)$$

E két feltétel egyezik a klasszikus fizikai megközelítésből következő kritériumokkal. Felmerülhet azonban az igény, hogy Kish eredeti, termodinamikai megfontolásokon nyugvó bizonyításához hasonlóan matematikai eszközökkel is bizonyítsuk, hogy léteznek feltételek, melyek *elégségesek* a rendszer abszolút biztonságosságához.

Mivel Eve által csak $V_{\mathrm{E}}(t)$ és $I_{\mathrm{E}}(t)$ mérhető, amennyiben a két mennyiség statisztikai paraméterein túl azok együttes eloszlása is megegyezik LH és HL állapotban, a kommunikáció abszolút biztonságos. A mennyiségekhez rendelt valószínűségi változók sűrűségfüggvényeivel ($p(I_{\mathrm{E}})$ és $p(V_{\mathrm{E}})$) és együttes sűrűségfüggvényével ($h(I_{\mathrm{E}},V_{\mathrm{E}})$) megfogalmazva a rendszer abszolút biztonságos, ha:

1. $p_{\mathrm{LH}}(I_{\mathrm{E}})=p_{\mathrm{HL}}(I_{\mathrm{E}})$,
2. $p_{\mathrm{LH}}(V_{\mathrm{E}})=p_{\mathrm{HL}}(V_{\mathrm{E}})$,
3. $h_{\mathrm{LH}}(I_{\mathrm{E}},V_{\mathrm{E}})=h_{\mathrm{HL}}(I_{\mathrm{E}},V_{\mathrm{E}})$.

Az (1) összefüggés szerint skálázott, normális eloszlású zajok esetén az első két feltétel teljesül. A 3. feltétel vizsgálatához elsőként numerikus szimulációkat készítettem LabVIEW környezetben. Egy bit átvitelét, azaz egy LH vagy HL állapotot az együttes eloszlások alakjának szórásdiagrammon való vizsgálatához a gyakorlati megvalósításhoz szükséges adatmennyiségnél jelentősen nagyobb, 2^{13} hosszúságú véletlenszámsorozatokkal vizsgáltam [1]. Normális eloszlás esetén a szóródási kép csak az (1) összefüggésnek megfelelő skálázás esetén volt megkülönböztethetetlen. Más stabilis eloszlások, illetve a véletlenszámgenerálás során elsődlegesen előálló egyenletes eloszlás esetén a megfelelő skálázást alkalmazva is megkülönböztethető volt az LH és HL állapot szórásdiagrammja. Ebből következően a normális eloszlástól eltérő valószínűség-eloszlások esetében, bár helyes skálázás esetén nulla a korreláció és a lineáris regresszió értéke, mégsem független a két mennyiség, egymásra vonatkoztatott regressziójuk nemlineáris, mely jól mutatja a normális eloszlás kitüntetett szerepét.

A biztonságosság elméleti vizsgálatához abból indultunk ki, hogy a 3. kritérium magától értetődően biztosított, ha V_E és I_E független, mely kitétel összhangban van Kish termikus egyensúlyt kihasználó bizonyításával [13].

Ez alapján, Lukacs és King 1954-es, független valószínűségi változók lineáris kombinációira vonatkozó tételét [16] felhasználva megmutattam, hogy V_E és I_E *akkor és csak akkor* független, ha a feszültségzajok normális eloszlásúak és az (1) egyenlet alapján megadott skálázási feltétel teljesül. Másszóval e két feltétel az abszolút biztonságosság *szükséges és elégséges* feltétele. Ezzel megadtam a KLJN protokoll abszolút biztonságosságának klasszikus fizikai megfontolásokat mellőző, de azokkal összehangban álló, matematikai alapú bizonyítását [1].

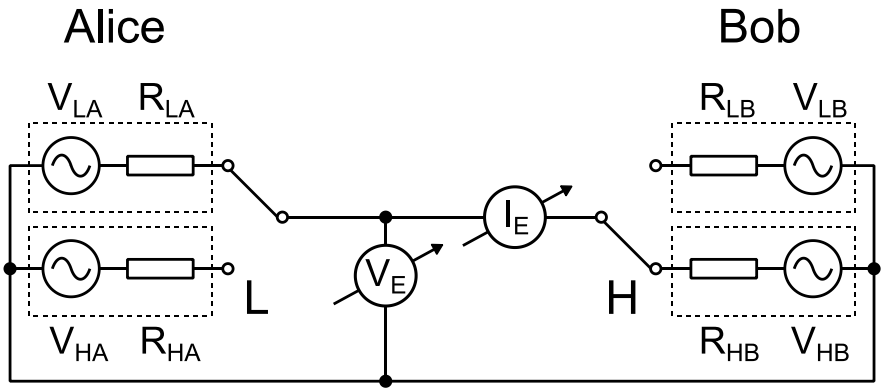
A KLJN kulcsmegosztó protokoll általánosítása

Normális eloszlású feszültségzajok esetén azok lineáris kombinációi, tehát V_E és I_E is normális eloszlású, így ez esetben azok függetlenségének megkötése egyenlő azzal, hogy a korrelációjuk nulla legyen. Rámutattam, hogy – mivel normális eloszlású feszültségzajok esetén V_E és I_E függőségét a korreláció teljes mértékben meghatározza – az is elegendő, ha a korreláció nem nulla, de azonos mértékű LH és HL esetben, hiszen ekkor Eve nem tud különbséget tenni a két állapot között [2]. Ez alapján a fentiekben meghatározott, abszolút biztonságossághoz tartozó három kritérium normális eloszlású zajokat feltételezve felírható az alábbi módon is:

1. $\left\langle I_{\mathrm{E,LH}}^2(t)\right\rangle = \left\langle I_{\mathrm{E,HL}}^2(t)\right\rangle$,
2. $\left\langle V_{\mathrm{E,LH}}^2(t)\right\rangle = \left\langle V_{\mathrm{E,HL}}^2(t)\right\rangle$,
3. $\left\langle I_{\mathrm{E,LH}}(t)V_{\mathrm{E,LH}}(t)\right\rangle = \left\langle I_{\mathrm{E,HL}}(t)V_{\mathrm{E,HL}}(t)\right\rangle$.

Mivel az első két kritériumnak megfelelő zajparaméterek esetén a korreláció az eredeti elrendezést vizsgálva LH és HL esetben nullának adódott, így egy

általánosabb rendszert vizsgáltunk: a 2. ábrán látható elrendezésben Alice és Bob két-két tetszőleges értékű ellenállást használ ($R_{LA} \neq R_{HA}$, $R_{LB} \neq R_{HB}$).



2. ábra: Az általánosított KLJN rendszer modellje (LH állapotban), négy különböző értékű ellenállás és effektív értékű zajgenerátor felhasználásával.

A négy zajgenerátorhoz négy valószínűségi változót rendelhetünk, melyek lineáris kombinációjaként a Kirchhoff-törvények segítségével felírhatjuk a vezetéken mérhető feszültséget és áramerősséget LH és HL esetben. Ezek alapján a három kritérium felírható az ellenállásértékek és zajgenerátorok effektív értékének függvényeként, mely egyenletrendszert megoldva a négy ellenállás és az egyik feszültségzaj varianciájának tetszőleges értékéhez megadható a másik három feszültségzaj varianciája úgy, hogy az abszolút biztonságosság kritériumai teljesüljenek [2].

Ezzel megmutattam, hogy a KLJN kulcsmegosztó protokoll abszolút biztonságos jóval általánosabb feltételek esetén is. A két kommunikáló fél által használt ellenálláspároknak nem kell azonos értékűnek lennie, megválasztható a zajgenerátorok effektív értéke úgy, hogy a lehallgató semmilyen módon ne tudjon különbséget tenni az LH és HL állapotok között. Ezt numerikus szimulációkkal is alátámasztottam; különböző aszimmetrikus elrendezéseket vizsgálva, 10^6 számú bitátvitel esetén $V_E(t)$ és $I_E(t)$ varianciái és korrelációja statisztikailag nem voltak megkülönböztethetőek. Eve hibás találati arányának (bit error rate, BER) vizsgálata ennek megfelelően nem mutatott információszivárgást [2].

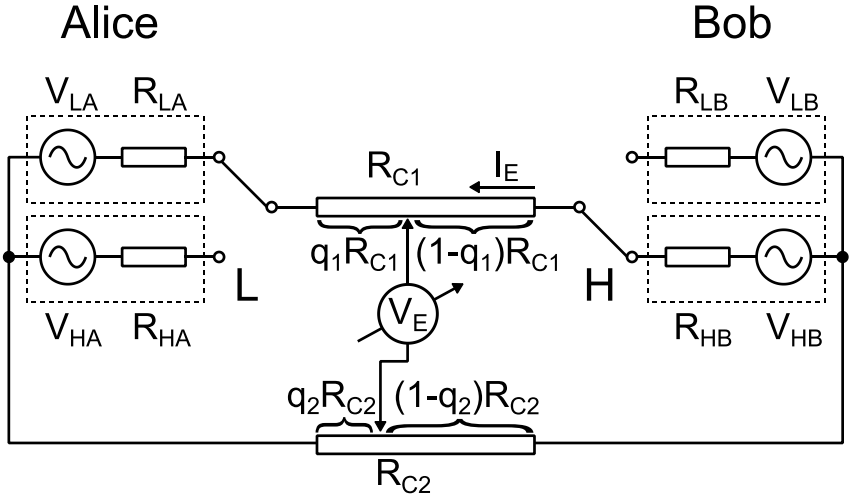
Ezen eredmények új megvilágításba helyezik a KLJN abszolút biztonságosságához szükséges követelmények klasszikus fizikai interpretációját is, hiszen az általánosított rendszer nincs termikus egyensúlyban, továbbá a nullától különböző értékű korreláció energiaáramlást jelent a két kommunikáló fél között. Az eredeti KLJN rendszer, melyben ez az energiaáramlás nulla, az általánosított rendszer egy speciális – szimmetrikus – esete. Ezen eredmények hatására Kish a protokoll biztonságosságának klasszikus fizikai leírását a termodinamika második főtétele helyett a fluktuáció-disszipáció tételét felhasználva újraértelmezte, továbbá eredményeink egy új protokoll bevezetésére is inspirálták [17].

Az általánosított rendszer jelentős előrelépést jelent a protokoll gyakorlati implementációjában, hiszen a komponensek tetszőleges értéke esetén beállíthatóak a zajgenerátorok úgy, hogy a kommunikáció abszolút biztonságos legyen.

Általánosított KLJN kulcsmegosztó rendszer gyakorlati alkalmazásokhoz

A KLJN rendszer gyakorlatban való alkalmazása szempontjából kulcsfontosságú kérdés, hogy a megvalósítás során az idealizált modellektől való eltérés milyen hatással van a rendszer biztonságosságára, ennek megfelelően a támadások jelentős része a nem-ideális rendszerre irányult. A nem elhanyagolható értékű vezetékellenállásából fakadóan például Eve következtetéseket vonhat le a különböző pontok közötti feszültégesésből vagy az energiaáramlásból. Amennyiben Alice és Bob ismeri Eve mérésének helyét és megméri a vezetékellenállás értékét, az előbbi eredményeink alapján a zajgenerátorok effektív értékét az abszolút biztonságosság kritériumainak megfelelően módosíthatja. Azonban valós esetben Eve mérési pontjának (vagy pontjainak) helyét nem ismeri a két kommunikáló fél, így felmerül a kérdés, mit tehet Alice és Bob a biztonságosság fenntartásához?

Ennek vizsgálatához az általánosított rendszert a 3. ábrán látható módon a kommunikációs és a referenciavezeték ellenállásával egészítettük ki, melyen Eve q_1 és q_2 relatív megfigyelési pontokban végez mérést.



3. ábra: Az általánosított KLJN rendszer modellje a kommunikációs vezeték R_{C1} ellenállásának és Eve q_1 megfigyelési pontjának, illetve a referenciavezeték R_{C2} ellenállásának és Eve q_2 megfigyelési pontjának figyelembevételével LH állapotban.

A vezetékellenállással kiegészített rendszer abszolút biztonságosságának zajparamétekre vonatkozó feltételeit az általánosított rendszer esetében alkalmazott eljáráshoz hasonlóan határoztam meg [3]. A rendszer biztonságosságához szükséges három kritérium, azaz V_E és I_E varianciáinak és korrelációjának egyenlőségét kifejeztem a feszültségzajok varianciáival, a komponensek ellenállásértékével és a megfigyelési ponttal, majd az egyenletrendszer megoldásával megadtam ezen értékek és az egyik feszültségzaj

varianciájának tetszőleges értékéhez a másik három feszültségzaj varianciájára vonatkozó formulákat [3]. Ez utóbbiakból látható, hogy a feszültséggenerátorok effektív értéke nem függ a megfigyelési ponttól, azaz nem kell ismernünk a lehallgató helyét, az abszolút biztonságosság a vezeték teljes hosszán garantált. A rendszer abszolút biztonságosságát numerikus szimulációkkal is igazoltam [3].

Az eredmények alapján a vezeték különböző pontjain eltér a feszültség és áramerősség korrelációjának értéke, azonban biztosítható, hogy ez megegyezzen az LH és HL esetekben. Ezzel értelmeztük a Kish által az eredeti rendszerre megadott kompenzációs eljárás [18] mérési ponttól való függetlenségét; a korreláció a szimmetrikus elrendezés esetén is csupán a vezeték közepén nulla, azonban semmilyen más ponton sem különböztethető meg a rendszer két állapota.

Az eredmény kiemelten fontos a gyakorlati megvalósítás szempontjából, hiszen, míg az eredeti rendszer esetében az implementációhoz szükséges alkatrészek információszivárgást okoztak, ezek a komponensek az új rendszer részét képezik ideális esetben is, amely a zajparaméterek megfelelő beállítása esetén abszolút biztonságos, így az általános védelmet nyújt a statikus esetben való támadásokkal szemben. Ehhez mindössze a komponensek pontos értékét kell ismerni.

Ezen ismeretek pontatlansága információszivárgást okoz, melynek mértékét numerikus szimulációkkal vizsgáltam [4]. Bár az információszivárgás mértéke függ az aktuális elrendezéstől, megállapítható, hogy a rendszer igen érzékeny a komponensek értékeinek pontosságára, azonban nagyságrendekkel érzéketlenebb a vezetékellenállás pontatlanságára. Mindazonáltal Alice és Bob könnyen módosíthatja – akár folyamatosan – a zajgenerátorainak effektív értékét úgy, hogy az információszivárgást eliminálja. Ehhez csupán meg kell mérnie a kommunikátorában található komponenseinek aktuális értékét, vagy akár a vezetéken mérhető jelekből is vonhat le következtetést a hiba kompenzálására.

3 Versenykajak mozgásjeleinek fluktuációanalízise

Periodikus folyamatok vizsgálata során a periódusidő vagy egy, a periódust jellemző mennyiség – akár véletlenszerű – ingadozása többletinformációt hordozhat; a mechanikus gépek periodikusan mozgó alkatrészeitől kezdve a szívműködésünk vizsgálatáig a variabilitás számos esetben hasznos diagnosztikai eszköznek bizonyult [19]. Napjainkban számos eszköz – mint például az okostelefon, óra vagy aktigráf – inerciaszenzorok segítségével képes a mozgás mérésére, így lehetővé válik a járás egyenletességének vagy napi aktivitásunk ritmusának vizsgálata is.

Ilyen típusú szenzorok használatosak a professzionális kajakos sportolók és edzők munkáját segítő eszközökben is, amely mozgás esetében ugyancsak az optimális mozdulatsor egyenletes megismétlése a cél. Az EDF Démász Szeged Vízisport Egyesülettel közösen indított projektben feladatunk a sportolók teljesítményének követésére alkalmas mérőrendszer fejlesztése volt [9].

Vizsgálataim során összefüggés mutatkozott a mozgás egyenletessége és a versenyzők technikai képzettsége között, így célkitűzésem a periódusfluktuációk és az evezés minősége közötti kapcsolat részletes elemzése volt.

A mozgásjelek mérése és az adatsorok osztályozása

A kutatócsoport által fejlesztett mérőrendszerrel a háromirányú gyorsulás- és szögsebességjeleket – a kommercionális eszközöknél jóval magasabb – 1000 Hz-es mintavételi frekvenciával mértük [9].

Egy sportoló aktuális teljesítményét számos tényező befolyásolhatja, ezért, hogy – amennyire lehetséges – az azonos körülmények között történő teljesítményeket vessük össze, 14 különböző korú és technikai képzettségű sportoló hosszútávú evezésének (>5 km) első 10 percét vizsgáltam.

Azzal a feltételezéssel élve, hogy a vizsgált evezéseken a sportolók átlagos teljesítménnyel és képzettségüknek megfelelő technikai kivitelezéssel eveztek, a mérőszámokat a technikai képzettség függvényében vizsgáltam, melyhez a sportolók életkorát, illetve a közreműködő edző által felállított, a technikai szint 1-től 10-ig terjedő osztályozást használtam fel.

Az időtartománybeli és spektrális fluktuációanalízisen alapuló indikátorok a jelek 30 másodperces időablakaira lettek kiszámítva, majd ezek 10 percre vett átlagai kerültek összehasonlításra.

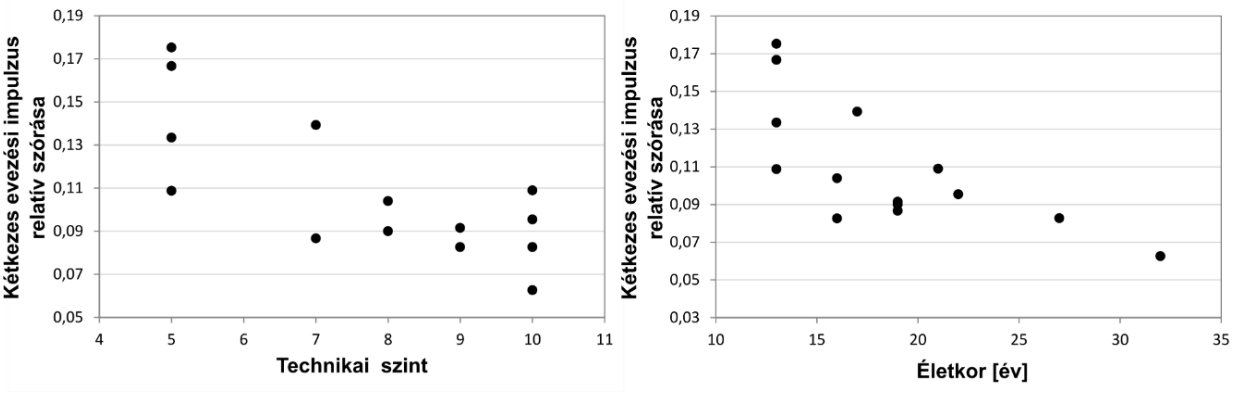
A mozgásjelek időbeli és spektrális fluktuációanalízise

A mért jelekből a mozgás pontos térbeli rekonstrukciója nem lehetséges, így a mozgásjelek periódusainak detektálásával és a jelalakok vizsgálatával szerezhetünk információt a sportoló evezéséről [20, 21]. Egy evezési periódust jellemző legfontosabb klasszikus paraméterek a *periódusidő*, az ebből számítható *csapásszám* illetve a húzást jellemző – a menetirányú gyorsulásgörbe pozitív szakaszának integráljaként számított – *evezési impulzus*.

Az evezési periódust jellemző mennyiségek statisztikai elemzésével rámutattam, hogy ingadozásuk mértéke kapcsolatban áll a sportolók technikai képzettségével, amely a 4. ábrán is megfigyelhető. A jelenséget jól demonstrálja a mennyiségek trendgörbéje illetve Poincaré-grafikonon való ábrázolása; egy serdülő versenyző mérőszámai jóval nagyobb mértékben ingadoznak, mint egy professzionális sportoló esetében [5]. E fluktuáció értelmezhető az alapján, hogy a kajak optimális előrehaladásához egyenletes evezés szükséges.

Ugyanakkor a periódusfluktuációkat jellemző szórás meghatározása során számos kérdés felmerül; normáljuk-e azt a mennyiségek átlagával, továbbá a mennyiségek trendszerű változása befolyásolja-e ezen értékeket? E kérdéseket a különböző módon számított indikátorok és a technikai szint, illetve az életkor közötti korreláció számításával vizsgáltam meg. Vizsgálataink a kajak mozgásának periodicitásán alapulnak, amely periódus a menetirányú gyorsulásjel alapján egy

evezésnek mutatkozik, azonban az evezés aszimmetriájából adódóan a mozgás teljes periódusa egy jobb- és egy balkezes evezés együttese, melyet eredményeim is alátámasztottak: minden szórás alapú indikátor esetén a kétkezes periódust leíró mennyiségek mutatnak erősebb kapcsolatot a technikai képzettséggel [6].



4. ábra: A kétkezes evezési impulzus relatív szórása a technikai szint edzői osztályozásának (bal oldalon) és a sportolók életkorának (jobb oldalon) függvényében.

A bemutatott variabilitás-vizsgálathoz a húzások detektálása szükséges, mely komplex jelalakok – például technikai hiba vagy sprintverseny – esetén igen nehéz feladat. Megvizsgáltam, hogy a nyers mozgásjelekből a periódusok azonosítása nélkül is kinyerhető-e a szükséges információ, így nem lenne szükséges az összetett és számításigényes detektáló algoritmus használata, továbbá eredményeinket nem befolyásolná annak megbízhatósága és pontossága.

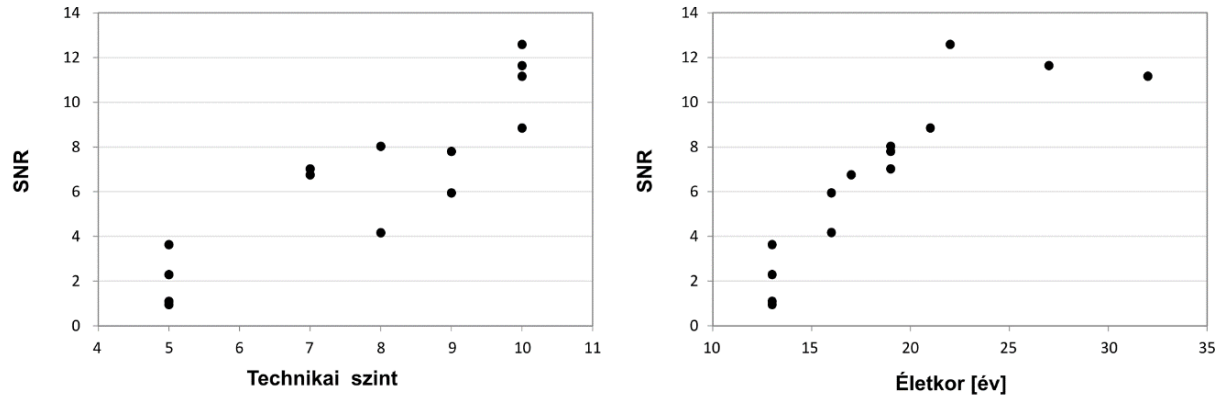
A mozgás egyenletessége frekvenciatartományban is vizsgálható, hiszen a mozgás periodikus komponenseit az evezési periódus által meghatározott frekvencia szerint szeparálhatjuk a többi jelkomponenstől, teljesítményük aránya pedig jellemezhető a *jel-zaj viszonnyal* (*signal-to-noise ratio, SNR*). A módszer további előnye, hogy nem kell a menetirányú gyorsulásjelre szorítkoznunk, mind a hat mozgásjel esetén kiszámíthatjuk indikátorainkat.

A jel-zaj viszonyon alapuló spektrális indikátorok meghatározásának alapvető kérdése, hogy hogyan definiáljuk a hasznos jelet és a zajt. A periodikus komponensek teljesítménye kapcsán teljesítménysűrűség-spektrumban figyelembe vett csúcsok meghatározásánál már az alapharmonikus kijelölése sem egyértelmű; a menetirányú és függőleges irányú gyorsulás illetve a billentési szögsebesség periódusa látszólag független a kivitelező kéztől, ez esetben a spektrumok domináns csúcsa az egykezes periódusidő által meghatározott frekvenciához (első felharmonikushoz), míg az oldalirányú gyorsulás, a csavarási és a forgatási szögsebesség domináns csúcsa a mozgás teljes, azaz kétkezes periódusideje által meghatározott frekvenciához (alapharmonikushoz) tartozik.

A mozgásjelek egy periódusának alakja meghatározza a teljesítménysűrűség-spektrumban a zajszintből jelentősen kiemelkedő felharmonikus csúcsok számát,

azonban az azok által megadott jelteljesítmény – például technikai hiba esetén – nem kizárólag az optimális mozgáskomponensekhez tartozik. A versenyzők evezéseire különböző számú felharmonikus figyelembevételével számított jel- és zajteljesítményeket és *SNR*-t a technikai képzettséggel mutatott determinációs együttható segítségével vetettem össze. Mivel a zajszintből kiemelkedő harmonikus csúcsok teljesítményének helyes meghatározása sem egyértelmű, ugyancsak megvizsgáltam a különböző numerikus módszerek – állandó vagy félértékszélesség alapú csúcsszélesség, felharmonikus kiszélesedés figyelembevételének, illetve Hanning- és Négyszög-ablak használatának – hatását is [6].

Az 5. ábrán a csavarási szögsebesség jel esetén az *SNR* és a versenyzők életkora, illetve technikai szintje közötti kapcsolat jól megfigyelhető.



5. ábra: A jel-zaj viszony (*SNR*) a technikai szint (bal oldalon) és az életkor (jobb oldalon) függvényében, a csavarási szögsebességjel esetén.

Az eredmények alapján a forgatási és csavarási szögsebességjelekre meghatározott mérőszámok mutatták a legerősebb összefüggést az evezés minőségével, azaz az időbeli vizsgálathoz hasonlóan ez esetben is a kétkezes periódusú mozgásjelek indikátorai karakterizálják legjobban az evezést [6].

A fluktuációanalízisen alapuló, újszerű megközelítés – mely alkalmasnak mutatkozik a technikai képzettség mérésére – számos további érdekes, nyitott kérdést vet fel: mik a periódusfluktuációk forrásai, milyen mértékben függ a fluktuáció a technikától, az abban jelentkező hibától, külső mechanikai effektusoktól vagy a fizikai és mentális állapottól? Milyen további indikátorok karakterizálhatják a technikai megvalósítást?

A periódusfluktuációk vizsgálata előremutató lehet más sportok és periodikus mozgásformák vizsgálatában, a teljesítmény értékelésében vagy egészségügyi paraméterek megállapításában. A periódusfluktuációkat jellemző időbeli és spektrális indikátorok közötti kapcsolat analitikus és numerikus módon is tovább vizsgálható. A jel-zaj viszonyon alapuló, spektrális variabilitás vizsgálat számos más periodikus – például élettani – jel esetén is hasznos lehet, hiszen nélkülözi az időtartománybeli periódus-detektálást, így ez a megközelítés aktuális kutatásaink tárgyát képezi.

4 Az értekezés tézispontjai

Az értekezésben bemutatott, a véletlenszerű fluktuációk hasznosításának témakörében elért új tudományos eredményeimet az alábbi négy tézispont foglalja össze, melyek végén megjelölésre kerültek az azokat alátámasztó publikációk. Az első három tézispont a zaj alapú abszolút biztonságos kommunikáció területén elért eredményeimet foglalja össze, melyek három nemzetközi folyóiratcikkben és egy konferenciacikkben jelentek meg. A negyedik tézispont a versenykajak periodikus mozgásjeleinek fluktuációanalízisével a sportolók teljesítményének értékelésére vonatkozó eredményeimet összegzi, melyeket egy meghívott előadáson alapuló nemzetközi folyóiratcikkben illetve egy nemzetközi konferencián mutattam be. Az alátámasztó közlemények típusát, illetve azok tézispontokkal való kapcsolatát az alábbi táblázat szemlélteti.

Tézis-pont	**Közlemények**					
	[1]	**[2]**	**[3]**	**[4]**	**[5]**	**[6]**
	Folyóirat Q3 IF=0,811	Folyóirat Q1 IF=5,228	Folyóirat Q1 IF=3,244	Konferencia	Konferencia	Folyóirat Q1 IF=2,196
1.	■					
2.		■				
3.			■	■		
4.					■	■

1. táblázat: Az értekezés új tudományos eredményeit összefoglaló tézispontok és az alátámasztó publikációk kapcsolata, jelölve a folyóiratok esetében azok impakt faktorát (IF) és a Web of Science rangsora szerinti minősítését.

1. A KLJN kulcsmegosztó protokoll abszolút biztonságosságához szükséges zajra vonatkozó követelmények bizonyítása

A KLJN protokoll matematikai statisztikai eszközökkel való vizsgálatának korábbi, a klasszikus fizikai megközelítéssel egyező eredményei alapján az abszolút biztonságos kommunikáció szükséges feltétele, hogy az alkalmazott zajgenerátorok által előállított feszültségzajok normális eloszlásúak legyenek, varianciájuk pedig az ellenállások aránya szerint skálázódjon. E vizsgálatot a lehallgató által a kommunikációs vezetéken mérhető áram- és feszültségzaj együttes eloszlásának vizsgálatával egészítettük ki. Először a rendszer numerikus szimulációjával demonstráltam, hogy a rendszer 0 és 1 értékű kulcsbiteknek megfeleltethető LH és HL állapotai a két említett feltételtől eltérő esetekben megkülönböztethetőek, azaz a kulcscsere lehallgatható. Ezután egy, két független valószínűségi változó lineáris kombinációinak függetlenségére vonatkozó tétel alapján megmutattam, hogy a

zajparaméterekre vonatkozó előbbi két megkötés a protokoll abszolút biztonságosságának szükséges és elégséges feltétele, ezzel megadva a protokoll biztonságosságának klasszikus fizikai megfontolásokat mellőző, matematikai bizonyítását. [1]

2. A KLJN kulcsmegosztó protokoll általánosítása

Az eredeti protokoll szerint a két kommunikáló fél azonos értékű ellenálláspárokat használ, a biztonságosság pedig a lehallgató által mérhető mennyiségek függetlenségén alapszik. Rámutattam, hogy az LH és HL állapotok megkülönböztethetetlensége ennél jóval kevesebb megkötéssel is biztosítható. Az áram- és feszültségzajoknak nem kell függetlennek lenniük, elegendő, ha e két mennyiség együttes eloszlása is megegyezik a két esetben. Ez alapján megmutattam, hogy normális eloszlású feszültségzajok esetén az abszolút biztonságosság kritériuma a vezetéken mérhető áram- és feszültségzajok varianciájának és korrelációjának egyenlősége LH és HL állapotban, mely teljesíthető egy jóval általánosabb rendszer esetén is, melyben mindkét fél tetszőleges ellenálláspárt használ. Az új kritériumok alapján formulát adtam a zajgenerátorok effektív értékeire, melyekkel az általánosított rendszer abszolút biztonságos. Eredményeimet numerikus szimulációkkal is igazoltam. Az eredeti KLJN rendszer annak a speciális, szimmetrikus esetnek felel meg, melyben a lehallgató által mérhető két mennyiség nem korrelál, azaz nincs energiaáramlás a két fél között, a rendszer termikus egyensúlyban van. A protokoll általánosításával rámutattam, hogy ez a megkötés nem szükséges az abszolút biztonságos kommunikáció megvalósításához. Ez a KLJN protokoll biztonságosságára vonatkozó klasszikus fizikai leírás újraértelmezését és új protokollok bevezetését eredményezte. Az új kulcsmegosztó protokoll, melyben a két kommunikáló fél rendszerének nem kell megegyeznie, jelentősen megkönnyíti a hardver megvalósítását és gyakorlatban való implementációját. [2]

3. Általánosított KLJN kulcsmegosztó rendszer gyakorlati alkalmazásokhoz

Az általánosított KLJN rendszer modelljét kiegészítettük a kommunikációs vezeték ellenállásával, melyen a lehallgató bárhol végezhet mérést. Megmutattam, hogy az abszolút biztonságosságot garantáló, a 2. tézispontban is alkalmazott feltételek ezen rendszer esetén is teljesíthetőek. Megadtam a feszültségzajok varianciájára vonatkozó formulákat, melyekből látható, hogy a zajgenerátorok biztonságossághoz szükséges effektív értéke nem függ a lehallgató megfigyelési pontjától. Az abszolút biztonságosság a vezeték teljes hosszán garantált; bár különböző pontjain eltér a feszültség és áramerősség korrelációjának értéke, azonban biztosítható, hogy az megegyezzen az LH és HL esetekben. Az eredeti rendszer esetén az ideálistól való eltérés, a vezeték és további, a gyakorlati megvalósításhoz szükséges komponensek ellenállása információszivárgást okozott. Ezzel szemben e komponensek az új rendszer részét képezik ideális esetben is,

amely a zajparaméterek megfelelő beállítása esetén abszolút biztonságos, így az általános védelmet nyújt a statikus esetben való támadásokkal szemben. Ez alapján a valós fizikai rendszerek komponensei által okozott hibát teljes mértékben, akár valós időben detektálni és kompenzálni képes protokoll jelentős mértékben megkönnyíti és elősegíti az eljárás gyakorlati alkalmazását. A rendszer biztonságosságát numerikus szimulációval is igazoltam, továbbá megvizsgáltam, hogy a valós implementáció során használt alkatrészek pontatlansága milyen mértékű információszivárgást okoz. [3, 4]

4. Kajakos sportolók teljesítményének értékelése a mért mozgásjelek fluktuációanalízisével

Kajakos sportolók evezésének vizsgálata kapcsán, a versenykajak mért mozgásjeleinek elemzése során megmutattam, hogy a mozgást jellemző periódusidő és a periodikus jelalakot jellemző evezési impulzus fluktuációja kapcsolatban áll az evezés minőségével, így az ingadozást jellemző időbeli, illetve a nyers mozgásjelek jel-zaj viszonyán alapuló frekvenciatartománybeli indikátorok többletinformációt hordozhatnak.

Az evezést, azaz a mozgásjelek egy periódusát jellemző klasszikus paraméterek értékének időbeli változását trendgörbéken és Poincaré diagrammon ábrázolva rámutattam, hogy azok ingadozása kapcsolatban áll a sportolók technikai képzettségével. Ezen kapcsolat vizsgálatához az evezési periódus és impulzus szórásán alapuló többféle indikátort, és a meghatározásukhoz szükséges numerikus módszert hasonlítottam össze. A legszorosabb összefüggést a mindkét kézzel történő evezési periódus evezési impulzusának relatív szórása mutatta.

A nyers mozgásjelek teljesítménysűrűség-spektruma alapján számolt jel-zaj viszonyon alapuló módszert vezettem be, melynek előnye, hogy nem kell az egyes periódusokat időtartományban detektálni, továbbá a menetirányú gyorsulás mellett a többi gyorsulás és szögsebesség jel fluktuációanalízise is lehetséges. Különböző jel és zaj szeparálási módszereket és az ezek meghatározásához szükséges számos különböző numerikus eljárást hasonlítottam össze mind a hat mozgásjel esetén. A mindkét kézzel való evezési periódushoz tartozó jelek esetén e kapcsolat jóval szorosabbnak mutatkozott.

Az indikátorok és a 14 különböző technikai képzettségű sportoló életkorának és edzői értékelésének korrelációja alapján kapcsolat mutatkozik a technikai képzettség és periódusfluktuációk között. Az eredmények számos érdekes, nyitott kérdésre világítanak rá, melyek további kutatások alapjául szolgálhatnak. A megközelítés más periodikus mozgások esetében is alkalmazható lehet, a variabilitás spektrális vizsgálata pedig további periodikus, például élettani jelek esetén is új eredményeket rejt magában. [5, 6]

5 Az értekezés alapjául szolgáló közlemények

[1] R Mingesz, G Vadai, Z Gingl, What kind of noise guarantees security for the Kirchhoff-Law-Johnson-Noise key exchange? *FLUCTUATION AND NOISE LETTERS* 13:(3) Paper 1450021, 7 p. (2014)

[2] G Vadai, R Mingesz, Z Gingl, Generalized Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system using arbitrary resistors. *SCIENTIFIC REPORTS* 5: Paper 13653, 7 p. (2015)

[3] G Vadai, Z Gingl, R Mingesz, Generalized attack protection in the Kirchhoff-Law-Johnson-Noise secure key exchanger. *IEEE ACCESS* 4: pp. 1141-1147 (2016)

[4] R Mingesz, N Bors, G Vadai, Z Gingl, Performance and security analysis of the generalized Kirchhoff-Law-Johnson-Noise key exchange protocol. *In Proceedings of 24th International Conference on Noise and Fluctuations (ICNF*) Vilnius, Lithuania, 2017.06.20-23. IEEE, pp. 200-203.

[5] G Vadai, Z Gingl, R Mingesz, G Makan, Performance estimation of kayak paddlers based on fluctuation analysis of movement signals*. In L Varani (ed.): Proceedings of 22nd International Conference on Noise and Fluctuations (ICNF)*, Montpellier, France, 2013.06.24-28. IEEE, Paper 6579010, 4 p.

[6] G Vadai, Z Gingl, Can the fluctuations of the motion be used to estimate performance of kayak paddlers? *JOURNAL OF STATISTICAL MECHANICS: THEORY AND EXPERIMENT* 2016: Paper 054040, 10 p. (2016), based on an invited talk presented at the 7th International Conference on Unsolved Problems on Noise, Barcelona, Spain, 2015.07.13-17.

6 Kapcsolódó közlemények

[7] R Mingesz, Z Gingl, G. Vadai, Security and performance analysis of the Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange protocol*. In Proceedings of 23rd International Conference on Noise and Fluctuations (ICNF)*, XI'An, China, 2015.06.2-5. IEEE, 4 p.

[8] LB Kish, Z Gingl, R Mingesz, G Vadai, J Smulko, CG Granqvist, Analysis of an Attenuator Artifact in an Experimental Attack by Gunn–Allison–Abbott Against the Kirchhoff-Law–Johnson-Noise (KLJN) Secure Key Exchange System. *FLUCTUATION AND NOISE LETTERS* 14:(1) Paper 1550011, 8 p. (2015)

[9] G Vadai, G Makan, Z Gingl, R Mingesz, J Mellár, T Szépe, A Csamangó, On-water measurement and analysis system for estimating kayak paddlers' performance. *In Proceedings of 36th Int. Conv., Microelectronics, Electronics and Electronic Technology*, Opatija, Croatia, 2013.05.20-24, IEEE, pp. 144-149.

7 Felhasznált irodalom

[10] C Shannon, Communication Theory of Secrecy Systems. *BELL SYSTEM TECHNICAL JOURNAL* 28:(4) pp. 656–715 (1949)

[11] CH Bennett, G Brassard, Quantum cryptography: Public key distribution and coin tossing. *In Proceedings of IEEE Int. Conf. Computers, Systems, and Signal Processing* Bangalore, India, 1984, pp. 175–179.

[12] LB Kish, Totally secure classical communication utilizing Johnson(-like) noise and Kirchhoff's law. *PHYSICS LETTERS A*, 352:(3) pp. 178–182 (2006)

[13] LB Kish, CG Granqvist, On the security of the Kirchhoff-law–Johnson-noise (KLJN) communicator. *QUANTUM INFORMATION PROCESSING* 13:(10) pp. 2213–2219 (2014)

[14] R Mingesz, Z Gingl, LB Kish, Johnson(-like)-noise-Kirchhoff-loop based secure classical communicator characteristics, for ranges of two to two thousand kilometers, via model-line. *PHYSICS LETTERS A* 372:(7) pp. 978–984 (2008)

[15] Z Gingl, R Mingesz, Noise properties in the ideal Kirchhoff-Law-Johnson-noise secure communication system. *PLOS ONE* 9:(4) e96109 4 p. (2014)

[16] E Lukacs, EP King, A Property of Normal Distribution. *THE ANNALS OF MATHEMATICAL STATISTICS* 25 pp. 389–394 (1954)

[17] LB Kish, CG Granqvist, Random-resistor-random-temperature KLJN key exchange. *METROLOGY AND MEASUREMENT SYSTEMS* 23:(1) pp. 3-11 (2016)

[18] LB Kish, CG Granqvist, Elimination of a Second-Law-Attack, and all cable-resistance-based attacks, in the Kirchhoff-Law-Johnson-Noise (KLJN) secure key exchange system. *ENTROPY* 16:(10) pp. 5223–5231 (2014)

[19] U Rajendra Acharya, K Paul Joseph, N Kannathal, C Lim, JS Suri, Heart rate variability: a review. *MEDICAL AND BIOLOGICAL ENGINEERING AND COMPUTING* 44:(12) pp. 1031-1051 (2006)

[20] DA Aitken, RJ Neal, An on-water analysis system for quantifying stroke force characteristics during kayak events. *INTERNATIONAL JOURNAL OF SPORT BIOMECHANICS* 8:(2) pp. 165-173 (1992)

[21] Z Ma, J Zhang, Y Sun, T Mei, Sports Biomechanical Information Acquisition and Evaluation for Kayaking Events. *INTERNATIONAL JOURNAL OF INFORMATION ACQUISITION* 6:(3) pp. 213-223 (2009)