

Kártyás beléptető rendszerek biztonsági vizsgálata

Szerző: Krisztián Dávid

(II. éves Villamosmérnök BSc hallgató)

Konzulens: Takács Szilárd László

Absztrakt

A 21. század szerves része az adatvédelem és önmagunk azonosítása, mely már a mindennapjaink részét képezi. Gondolhatunk itt a telefonon való bejelentkezésre is, mely ujjlenyomatot, esetleg arcfelismerőt alkalmaz identitásunk megerősítése képpen. A dolgozat témája az RFID-s (Radio Frequency IDentification) rendszerek, amelyeket cégeknél és nagyobb intézményeknél kártyás beléptetésként, logisztikai iparban, kereskedelemben áru-nyomonkövetés formájában, illetve járművekben immobiliser (lopásgátló), háziállatokban „csip” néven, beültetve egyfajta rendszámként, a tulajdonos beazonosítása végett alkalmaznak. A fő kutatási terület a beléptetőrendszereket ismerteti részletesebben, amely egy jól bevált, egyszerű, kézzel fogható módja az épületekhez, rendezvények különböző területeikhez való hozzáféréséhez. Egy ilyen infrastruktúrával hosszútávon jelentősen csökkenthetők az üzemeltetési költségek, például kevesebb alkalmazottra van szükség a biztonság fenntartásához és gyorsítható a belépési folyamat.

A dolgozat taglalja, hogy hol találkozhatunk ilyen technológiával a mindennapjainkban és milyen gyakran, szinte észrevétlenül körbevesz minket. A technikai, fizikai részletekre nagyobb hangsúlyt fektetve, például többek között, hogyan kommunikál az olvasó egy címkével, milyen modulációs eljárásokat alkalmaz az RFID az adatátvitel megvalósításához alapesetben kettő, de lehet akár három vagy több fél között is, illetve különböző frekvencia-tartományokban hogyan változik a belső felépítés struktúrája. A tanulmány célja, hogy egy meglévő rendszer működését körüljárja, nagyobb hangsúlyt fektetve annak kritikus pontjaira, többek között: nincsenek védve a kártya adatai, így bárki hozzáférést nyerhet, támadási felületeire: oszcilloszkópos mérés alapján lehallgatható a „tag” és az olvasó közötti kommunikáció majd a kockázatos részeknek a kielemezése révén a biztonság növelése céljából (alap, illetve akár fejlettebb titkosítási módszerek használatba vételére) javaslatokat tegyen.

Tartalomjegyzék

Absztrakt.....	2
1. Bevezetés	4
2. Átfogóbb ismeretek a technológiáról	4
2.1. Rövid történelem.....	4
2.2 . Mindennapi alkalmazási területek.....	6
2.3 NFC az RFID-ben.....	8
3. Fizikai felépítés	9
3.1 Tagek.....	9
3.2 Olvasók	13
4. Széchenyi István Egyetem beléptetőrendszerének tesztelése.....	16
4.1 tag-ek (címkék) adatvédelme, sokszorosíthatósága	16
4.2 Hallgatózás	20
Konklúzió	27
Irodalom.....	28

1. Bevezetés

A technológiai innovációk általában megkönnyítik a mindennapokat, hiszen azért folynak a fejlesztések, kutatások, kísérletezések, hogy például: egyszerűbb, gyorsabb, hatékonyabb legyen elvégezni a munkát egy gyorsabb lappal. Gyorsan kitakarítható legyen az egész ház egy csendesebb, vezeték nélküli porszívóval. Közlekedni A-ból B-be költséghatékonyabban, fele annyi üzemanyagot elhasználva egy hibrid autóval. Vagy csak egyszerűen bemenni a munkahelyre, strandra, az egyetemre egy kártyát az ajtónál leolvasva és már is sűrűlőds mentesen közlekedhetünk az épületek között.

Manapság az életünket nehezen lehetne elképzelni valamilyen féle azonosítási módszer nélkül, legyen az bár milyen igazolvány, ujjlenyomat, arc, a klasszikus felhasználónév – jelszó páros vagy éppenséggel egy gyors érintéses vagy megközelítéses módszer (RFID-**R**adio **F**requency **I**Dentification), mintha csak intenénk a portásnak, aki már ismer minket, és nyitná is az ajtót.

A dolgozat fő témája az utóbbiként említett azonosítási módszer, többek között ki fog térni olyan területekre, mint például: hol találkozhatunk ezzel a technológiával a mindennapjainkban és hogy milyen gyakran és szinte észrevétlenül körbevesz minket, az ipar és a kereskedelem hogyan használja fel ezt a technológiát, hogyan működik egy ilyen rendszer, milyen felépítése van a címkéknek („tag”-eknek), hogyan működik a vezeték nélküli áramellátásuk, milyen frekvenciatartományú jeleket, titkosítási módszereket, modulációs eljárásokat használnak, hol és milyen mennyiségben tárolják az információt. És végül, de nem utolsó sorban, kísérletek címkék sokszorosításával, személyre szabásával és a két fél közötti rádiós kommunikáció lehallgatásával.

2. Átfogóbb ismeretek a technológiáról

2.1. Rövid történelem

Az RFID (**R**adio **F**requency **I**Dentification) története egészen a második világháborúig vezethető vissza, sok más találmányhoz hasonlóan. Mindenki radarokat használt, hogy figyelni tudják a repülőgépek helyzetét a légtérben, a probléma ott ütötte fel a fejét, hogy az összes detektált jel egyforma volt és csak egy repülő jelzett, több információval nem szolgált, így nem tudták megkülönböztetni a szövetséges gépeket az ellentől.

Két lényeges mérföldkő a történelemben: az egyik 1970-ben, Mario Cardullo levédette a memóriával ellátott, aktív válaszjeladó eszközt (transzponderét), amely fény és hangjelzés útján is kommunikált a rádióhullámok mellett. Sokan ezt tartják a mai RFID címkék igazi ősenek. A második 1973-ban három kutató (Steven Depp, Alfred Koelle és Robert Freyman) szemléltette, rádió-frekvenciás sugárzást moduláltan visszaverő passzív és fél-passzív címkék működését. A hordozható rendszer 12 bites adattárolási kapacitással bíró címkéket és 915 MHz-es frekvenciát használt, amelyre a mai UHF (Ultra High Frequency) RFID címkék is épülnek.

Az első szabadalom formájában megjelent feljegyzés a technológiáról, amely tartalmazta az RFID kifejezést Charles Walton amerikai feltaláló jegyeztette be 1983-ban. Ezt követően továbbra is tevékenykedett, így a szakterületen tíz további szabadalom fűződik a nevéhez.

Az amerikai kormány szintén dolgozott hasonló rendszereken, a hetvenes években felkérték a Los Alamos-i nemzeti laboratóriumot, hogy fejlesszenek egy követő rendszert a nukleáris anyag-szállítmányozáshoz. Egy maréknyi tudós azzal az ötlettel állt elő, hogy elhelyeztek válasz-jeladókat a teherautókon és olvasókat a magas biztonságú létesítmények belépési pontjainál, amikor megérkezett a rakomány a kapunál folyamatos jelet sugárzó olvasó felébresztette a jeladót, az pedig egy azonosítóval válaszolt és akár egyéb információkkal, például a sofőr jelkódjával. Ez a rendszer a 80-as évek közepére kereskedelmi forgalomba került, miután a korábban említett tudósok kiváltak a laboratórium intézményéből és saját céget alapítottak, hogy automatizált útdíjfizetési rendszereket fejlesszenek. Ez a későbbiekben elterjedté vált autópályák, hidak és alagutak széles körében.

A mezőgazdasági szektor kérésére a Los Alamos-i laboratórium kifejlesztett RFID rendszert a tehenek nyilvántartására (1. ábra). Az volt az alapvető probléma, hogy a jószágok időszakosan kaptak gyógyszereket és nehéz volt nyomonkövetni, hogy minden tehén a megfelelő dózist kapja, illetve nem lett-e kétszer beoltva. Erre készült egy passzív címkés



1. ábra: tehenek fülére rögzített RFID címke (Herdx, 2024).

egység, ami UHF rádióhullámokat használt. A címke az energiáját az olvasóból nyerte majd szimplán visszareflektálta a modulált jelet (Roberti, 2005).

2.2. Mindennapi alkalmazási területek

A technológia egyik legnagyobb felhasználója a kereskedelem, Magyarországon 2021 január elsejétől kötelezővé vált az online pénztárgépet üzemben tartó kereskedők számára legalább egy elektronikus fizetőeszköz biztosítása a vásárlók részére (Pál, 2021). Ezáltal és az akkori járványügyi intézkedések által még nagyobb löketet kapott az érintésmentes bankkártyás fizetés elterjedése. Napjainkban odáig jutottunk, hogy a legutolsó kávé vagy üdítő automatát is ki lehet fosztani egy bankkártyával, így elkerülhető az, hogy aprópénzt kelljen felváltatni ilyen eshetőségekre.

A kártyáink és a bankszámláink mára elége kifejlett biztonsági rendszerekkel és egyéb többfaktoros azonosítási módszerekkel vannak biztosítva, példának: a POS (Point of Sale) terminál és a kártya közötti kommunikációt (2. ábra) az EMV chippek (EMVCo, 2024) és szabványok biztosítják (amit a MasterCard és a Visa közösen fejlesztett ki egy egységes standardizált technológia létrehozása céljából).



2. ábra: érintés mentes fizetés

Ha elveszne egy kártya maximum 15 ezer forintig lehet róla vásárolni, utána a terminálnál pinkód megadása szükséges, bár ezt megelőzően szinte azonnal le is lehet tiltani netbankból. Legszélsőségesebb esetben egy vezeték nélküli terminált zsúfolt tömegben táskához, pénztárcákhoz, zsebekhez érintve sem lehetne „fosztogatni”, hiszen a tulajdonosa ismert, illetve a bank birtokában áll minden információ a tranzakciókat illetően.

Egyre több üzletben találkozhatunk vagy éppen nem, mert első ránézésre nem is gondolnánk, hogy a termékekbe vagy a csomagolásukban van elrejtve egy biztonsági funkciót ellátó RF címke, például belevarrva ruhák bilétájába (3. ábra, ezt akár egy zseblámpával ellenőrizhetjük), a vonalkód levonójába a papírréteg alá beleragasztva. Ezeknek 2 fajtáját különböztetik meg: a mikrohullámú (UHF) frekvenciás passzív (EPC – Electronic Product Code) típusú, ezekre az információk egyszer vagy gyártáskor kerülnek beírásra, többször

olvashatók és rendelkeznek „kill”¹ paranccsal. Az egyszerűbb szintén passzív, de magas frekvenciás (HF) és vagy alacsony frekvenciás (LF) rezonancia alapon működő típusok, amik semmilyen információt nem tárolnak csak a szimpla jelenlétüket érzékelik a boltok kijáratánál elhelyezett, ember magasságú műanyag oszlopok. Mindhárom típust megfelelően erős elektromos tér semlegesíteni tudja, így vásárlás (vagy kiiktatás) (Staff, 2014) után már nem kerülnek újra detektálásra és nem okoznak kellemetlen szituációt.

Egyes áruházakban az RFID nem csak áru-védelmi célokra, hanem vonalkód helyettesítő alternatívaként kerül alkalmazásra, (3. ábra, ilyen hazánk egyik közkezdelt



3. ábra: UHF RFID „tag” szövet ruhacímkébe integrálva előről, hátulról és átvilágítva

sportáruháza is). Működési elve pontosan ugyan az. Egyedüli különbséget a címkék detektálása képez, ami kizárólag egy zárt térben történik. (Maulana, 2021) (a doboz, amibe elhelyezésre kerülnek a megvásárolni kívánt termékek) Egynél több címke jelenléte esetében felmerül a kérdés, hogyan „hallgassuk ki” mindegyiket, úgy, hogy ne legyenek időbeli ütközések az információ folyamában. Erre megoldásként réselt ALOHA protokollt alkalmaznak.

Beléptető rendszerek esetén már nincs egyetlen egyértelműen kimondható szabvány, az egységesség körülbelül húsz ISO (International Organization for Standardization – Nemzetközi Szabványügyi Szervezet) által kiadott szabványban van megfogalmazva, a legkézzelfoghatóbb kategorizálása a fent említett frekvenciasávok által megadott csoportokra bontható. (ISO 18000-V1-től V7-ig, ez a 7 szabvány lépcsőzetesen magában foglalja a 135kHz-től 5.8GHz-ig terjedő skálát).

¹ minden funkciót semlegesítő parancs

Autós körökön kívül sokak számára ismeretlen a tény, hogy a 1998-után gyártott személygépjárművek (kivéve egyes koreai márkák 2011 és 2021 között gyártott darabjait) immobiliser (indításgátló) rendszerrel vannak ellátva, ami meggátolja az autó indítását (legalább kettő) a gyújtás-elektronika és az üzemanyag rendszer inaktíválásával.

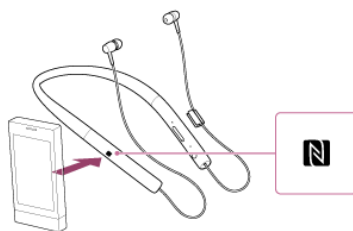


4. ábra: Immobiliser csipek

Tipikusan a 125 kHz-es (LF - Low-Frequency) frekvenciasávot használják, működési elvük ugyan az, mint a kártyás rendszereknél. A kulcsban van egy antennával ellátott transzponder, (4.ábra) ami az energiáját a kormányoszlop közelében lévő olvasótól nyeri. Ha az immobiliser nem érzékel vagy nem a hozzátársított jeladó van a közelben akkor meggátolja az autó indítását még akkor is, ha van a gyújtáskapcsolóban egy tökéletes másolat a fizikai kulcsról, vagy a kapcsolót megkerülve „elkötnék” a járművet.

2.3 NFC az RFID-ben

A mozaikszóból (Near Field Communication - rövid hatótávolságú kommunikáció) adódik, hogy ennél a rendszernél kétirányú adatfolyam formájában történik információ csere. A hangsúly két eszköz közötti gyors, egyszerű kapcsolatfelvételre és a bővített funkciókra, üzemmódokra került, RFID író-olvasóként: okos címkék, interaktív poszterek programozhatók, amik leolvasáskor műveletsorokat is végrehajthatnak egy telefonon (pl.: megnyitnak egy alkalmazást, weboldalt), emulálóként egyes esetekben hozzáférés szabályozására (beléptetésre), de leginkább bankkártya helyettesítése a leggyakoribb felhasználási eset. Végül a fentebb említett NFCIP Peer-to-Peer (pont-pont) kommunikáció alkalmazása. Bár az adatátvitel sebessége elég alacsony 106-412 kBit/sec, (Mulliner, 2011), ez pont elég arra, hogy másodpercek alatt beléptetési információt cseréljünk két telefon között WiFi hálózatra



5. ábra: illusztráció (Sony, 2021)

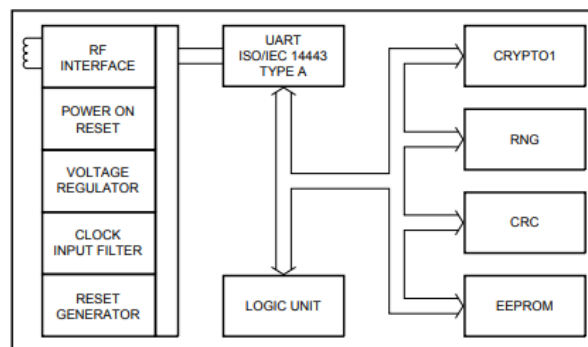
csatlakozás céljából vagy lehetővé téve egyérintéses csatlakozást Bluetooth eszközhöz (5.ábra), ezzel kiváltva a nehézkes és sokszor problémás párosítási folyamatot. A kommunikáció NDEF (NFC Data Exchange Format) üzenetek formájában történik. A jelátvitel Manchester kódolást és ASK (Amplitude Shift Keying) modulációt használ. mivel a rádiós kommunikáció alapesetben nincsen titkosítva ezért az egyetlen védelmet a pár centiméteres olvasási távolság adja, ami önmagában elég is, viszont továbbra is fennáll a lehetsége Man-in-the-middle támadásnak (az eredeti jel elfogása majd továbbítása a támadó céljai szerint módosítva), megfelelő antennával lehallgatás is kivitelezhető, maximum egy-két méterig. Legkönnyebben módosítással támadhatóak meg a passzív eszközök, azonos megjelenésű de más információkat tartalmazó címkéket felülmatricázással, nem megfelelően felprogramozottakat pedig egyszerű újraírással.

3. Fizikai felépítés

A továbbiakban nagyrészt a MIFARE Classic kártyák specifikációi (NXP, 2017) szerint folytatódik a dolgozat. (Ez a rendszer ihlette a kutatás és további ismeretek szerzésének vágyát, nem utolsósorban a világ azonosító rendszereinek kb. több mint 70%-a valamelyik Mifare technológiát használja.)

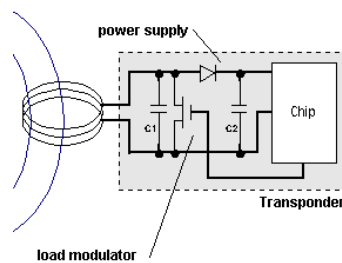
3.1 Tagek

A fő komponense minden címkének az integrált áramkör, ami tartalmazza a kommunikációs, tápellátási, logikai, adattárolási (memória) és titkosítási feladatokat ellátó egységeket.



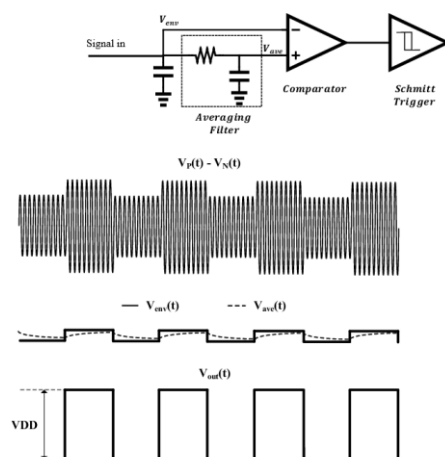
6. ábra: MIFARE CLASSIC integrált áramkör blokk diagrammja (NXP, 2017)

A rádiófrekvenciás egység felel a külvilággal való kommunikációért (6.ábra „RF interface” oszlopa), adatok továbbításért belső egységek felé, tápellátás stabilizálásáért. Erre kapcsolódik az antenna, ami a rádió-frekvenciás áramkörrel van közvetlen kapcsolatban. A bejövő jel először egy AM (Amplitúdó Modulációs) detektoros rádió kapcsoláson keresztül halad át, ami egy nagyfrekvenciás diódából és egy vele sorbakötött kondenzátorból áll. (7.ábra „power supply” felirattal jelezve) Leszűri a váltakozó áramú komponenseket és egyfajta pufferként kisimítja a nagyobb ingadozásokat, így a feszültség-szabályzó stabilabb tápellátást tud biztosítani a többi rész egységnek és a beérkező jel is demodulálhatóvá válik. Ezután a jel egy komparátoros-Schmitt triggeres kapcsolással demodulálásra kerül (8.ábra), ezzel párhuzamosan leszűri az órajelet. A demodulált és órajellel ellátott információt UART-on keresztül, (ami bejövő adatokat aszinkron start-stop bitekkel határolt bitfolyammá konvertálja,)



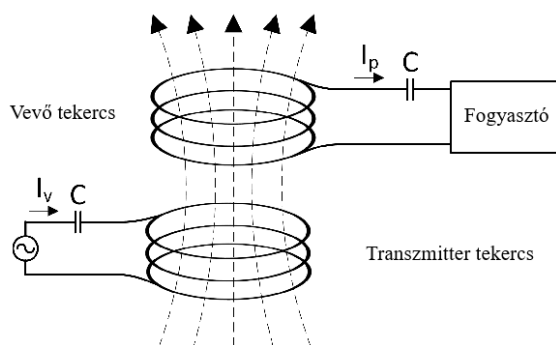
7. ábra: címkek adó-vevő áramköre (Finkenzeller, 2010)

így már fel tudja dolgozni a logikai vezérlő, ami szükség esetén elvégzi a dekódolás procedúráját, elraktározza az információt, ír-olvas az EEPROM memóriából vagy visszaküld adatokat az olvasó felé a vivőfrekvencia terhelés-modulációjával, az antennával párhuzamosan kapcsolt MOSFET segítségével. (7.ábra „load modulator” felirattal jelezve)



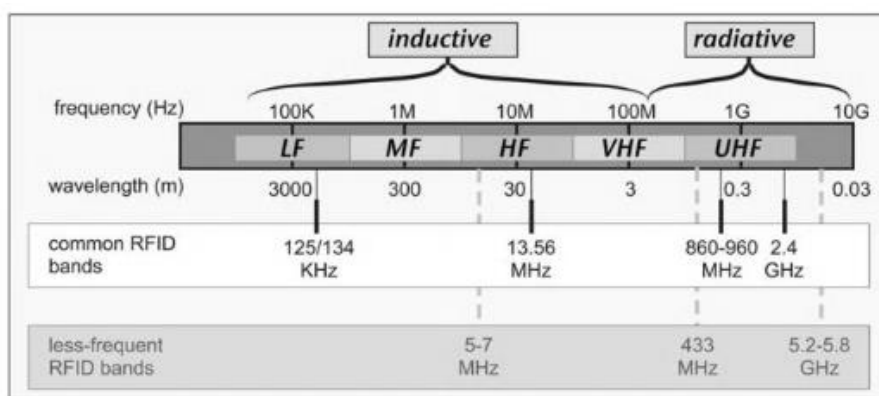
8. ábra: órajel visszaállító kapcsolás (Hamed Rahmani, 2020)

A rádiófrekvenciás egységhez két kivezetésen keresztül kapcsolódik a külső antenna, ami a használt frekvenciasávától függően más-más kialakítást igényel (10.ábra). Alacsony (LF)



9. ábra: induktív csatolás (Dobkin, 2007)

frekvenciáktól magas (HF) frekvenciáig induktív csatolást alkalmaznak (9.ábra). Működési elvét tekintve, a két vezető (antenna tekercs) úgy van kialakítva, hogy az egyik tekercsben folyó áram elektromágneses indukció révén feszültséget indukál a környezetében lévő másik tekercs két kivezetésén, ezáltal lehetséges, vezeték nélküli energia és moduláció segítségével digitális (0-1 szintű) információ átvitele.



10. ábra: RFID által használt frekvenciák (Dobkin, 2007)

Alacsony hullámhosszú (LF) frekvenciák esetében, klasszikus, sokmenetes (kb. ~100) induktív tekercs szolgál a jel felfogására és visszasugárzására. Hátránya, hogy egyes kivitelek érzékenyebbek mechanikai behatásokra. Például az üveg kapszulás megoldások törékenyek (előfordulnak: régebbi immobiliserek, háziállatokban „csip” néven ismert implantátumok formájában), hajlékony kártyában nem lehetnek beragasztva mert a tekercset alkotó réz-drót egy idő után a különböző behatásoktól megtörne.

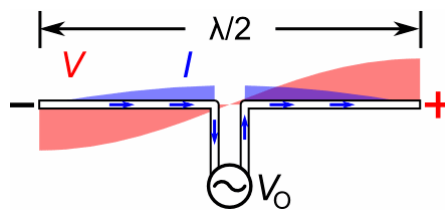
Magas (HF) frekvenciákon (konkrétan 13,54 MHz-en) még szintén induktív csatolást alkalmaznak, viszont sokkal kevesebb menettel rendelkező tekercsek (kb. 5-10) elegendőek a kívánt induktivitás eléréséhez (L induktivitás kiszámolása, ahol N : menetszám, l : a tekercs hossza, μ_0 : vákuum permeabilitása, μ_r : tekercsbe helyezett mágneses anyagra jellemző szórószám, A tekercs keresztmetszete).

$$L = \frac{\mu_0 \cdot \mu_r \cdot A}{l} \cdot N^2$$

általános szabály: ahogy nő a frekvencia annál kisebb értékekkel valósítható meg egy rezgőkörös kapcsolás az antennák rezonancia frekvenciára hangolás miatt. (f_0 rezonancia frekvencia kiszámítása).

$$f_0 = \frac{1}{2 \cdot \pi \cdot \sqrt{L \cdot C}}$$

Mikrohullámú (UHF) sávban az energia és jelátvitel sugárzásos (radiative) elven történik. Általában dipólusú antennát használnak (11.ábra). A hatékony működéshez elég a

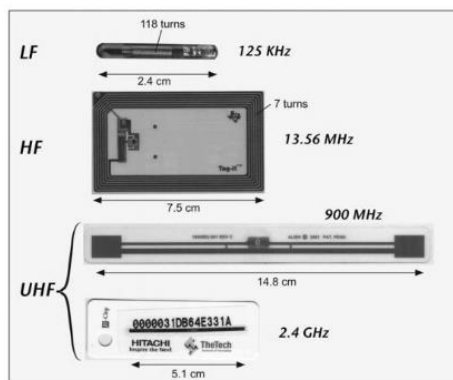


11. ábra: dipólantenna működési elve

használt frekvencia hullámhosszának a negyedével megegyező hosszúságú vezető anyagból elkészíteni az antenna két kivezetését. A két negyed pontosan egy fél-hullámhosszú vezetőt alkot, amiben a 11.ábra szerint változik a feszültség $V(t)$ és az áram $I(t)$ az idő függvényében. A λ hullámhosszt a rádióhullámok c terjedési sebessége (fénysebesség) és az f frekvenciájának a hányadosa adja (3.képlet).

$$\lambda = \frac{c}{f}$$

LF „tag”-ek nagyrészt kialakításuk miatt masszív formában fordulnak elő, például vastag plasztik kártya, epoxy gyantával kiöntött műanyag házban. HF és UHF „tag”-eket lényegesen egyszerűbb bármibe beleintegrálni a kevés vagy nélkülözhető menetszám miatt,



12. ábra: tag”-ek frekvenciatartomány alapján változó felépítése (Dobkin, 2007)

ezáltal legyen az kártya, korong alakú kulcstartó, hajlékony, papírvékony matrica kivitelben is megvalósíthatóak amire tetszőleges ábrákat, szöveget is lehet nyomtatni.

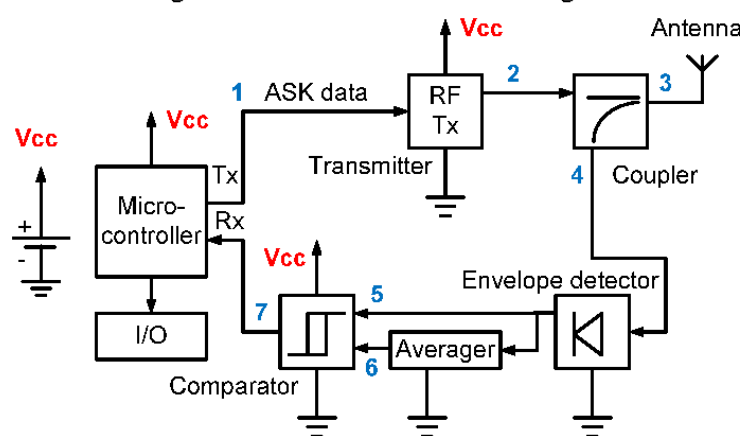
3.2 Olvasók

A „tag”-ek ellenpárjaik, feladatuk: hozzáférjenek és kinyerjék a címkékben tárolt információkat. Az olvasási eljárás során egy kérést küldenek a „tag”-ek felé. Az olvasó által generált elektromágneses mezőt az antennákon keresztül felhasználja a címke az áramkörének energia ellátására, hogy hozzáférjen az elraktározott adatokhoz és visszaküldje az olvasónak. Ezt a folyamatot „backscattering”-nek (angolról fordítva, visszaszórásnak) nevezzük.

A három fő frekvenciasávra felosztás a címke-olvasóknál is érdemes alkalmazni. LF és HF olvasók vegyesen előfordulnak fixen telepített és hordozható formában. LF rendszerek jobban teljesítenek zavaros közegekben. Fémek, folyadékok környezetében rövid, pár centiméteres üzemi távolsággal dolgoznak. HF esetében nagyobb hatótávval számolhatunk, akár egy méterig. Az UHF sávban üzemelőkre jellemző a stacionárius elhelyezés, a nagyobb kommunikációs távolságok (pár méter) kihasználása miatt (útdíj ellenőrzési rendszerek, mozgó vasúti kocsik azonosítás, bolti, könyvtári lopásgátlók környezetében).

	Maximális effektív hatótávolság (m)		
	(-30°) szögben	Merőlegesen	(30°) szögben
865.6-867.6 MHz	6.4	7.5	6.5
902.75-927.75 MHz	6.3	7.3	6.3
952 MHz-954 MHz	6.1	7.1	6.1

1. táblázat: UHF olvasók hatótávolsága

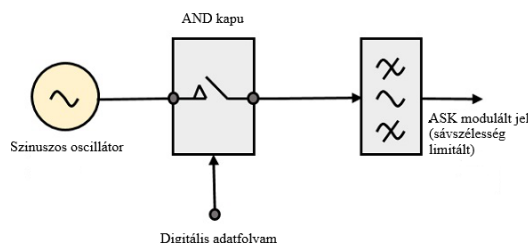


13. ábra: RFID olvasó blokk diagramm (P. Nikitin, 2013)

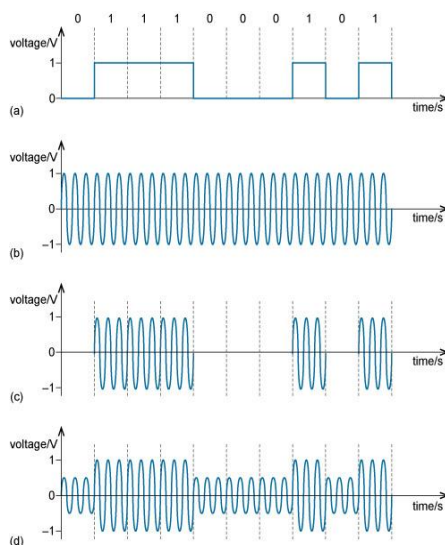
A blokkdiagramm (13.ábra) sok hasonlóságot hoz a címkékhez viszonyítva. Itt is megtalálhatóak a következő kapcsolások: a vételi (Rx - Receiver) oldalon történik a jel demodulálása egy Schmitt triggeres és az AM detektoros kapcsoláson (envelope detector-on) keresztül.

Újdonság képpen megjelent a MOSFET helyett egy transzmitter, és az I/O blokk. A transzmitter, egy ASK modulátort (14.ábra) tartalmaz. Az ASK (Amplitude Shift Keying) moduláció a következő képpen működik. Egy oszcillátor szolgáltatja az alapjelet (vivőfrekvenciát). A folyamatosan oszcilláló jelet a digitális adatfolyam modulálja, amikor logikai 1 érték érkezik akkor a kimeneten sokkal magasabb amplitúdójú lesz a jelalak, mint amikor logikai 0 az speciális ÉS kapu (14.ábra, AND kapu) bemenetére. Ez azért speciális mert az alapjelet a moduláció szintjének függvényében (100%-ot kivéve) részlegesen átereszt, hogy folyamatosan fennmaradjon a térerő (15.ábra).

Az olvasók nem „zsákutcaként” üzemelnek, a mikrokontroller I/O-jai (Input/Output) által képesek kommunikálni külső számítógéppel és egymással is. Hálózatba köthetők WiFi-n, ethernet keresztül, számítógéphez csatlakoztathatók USB-n és soros porton keresztül (pl. RS-232, RS-485). Egyszerűbb automatizálási feladatokat is képesek ellátni (forgókapun beléptetni, mágneszárat, sorompót nyitni), megfelelő számítási kapacitás feltétele mellett, például



14. ábra, ASK moduláció blokk diagramm

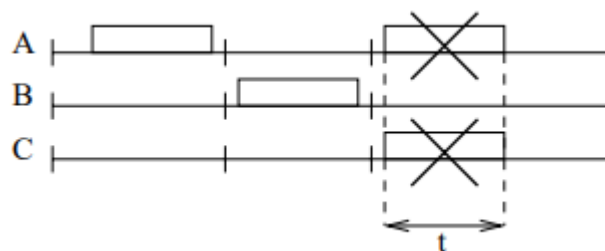


15. ábra, ASK modulált jel összetétele
(OpenUniversity. 2024)

beléptető rendszer esetében bekérhet további azonosítási módokat is (PIN-kódot, biometrikus adatokat).

Több résztvevős kommunikációs rendszer bevezetésével új problémák merültek fel: a közeghozzáférés szabályozásának szükségessé válása. Két félélt különböztetünk meg, egyik a címke ütközés. Ilyen abban az esetben történhet amikor egy olvasó hatósugarában egyszerre több „tag” van jelen. A másik amikor több olvasó próbál egyszerre több címkével adatcserét folytatni (általában UHF, mikrohullámú rendszereknél fordulhat elő a nagy hatótávolságok miatt, ezért erre az esetre a dolgozat csak dióhéjban fog kitérni), ez előfordulhat raktárakban, ahol jelen van egy folyamatosan üzemelő, fixen telepített, nagy hatósugarú, készlet nyilvántartási célra használt RFID állomás, amivel interferálhat a targoncás kézi kereső pisztolya.

Az ütközések elkerülhetetlenek több kártya, címke azonos időbeni jelenléténel. Nagy valószínűséggel fordulnak elő ilyen esetek ezért közeghozzáférési protokoll alkalmazására van szükség. Amíg az olvasó összegyűjti a jelenlévő címkék azonosítóit addig réselt ALOHA protokollt használ. Hierarchiát tekintve *master-slave* (mester-szolga / olvasó-címke) az alárendeltségi viszony a felek között. A *mester* figyeli a kommunikációs csatornát és ha hibátlan adatkeretet vesz (sikeresen megkapja a *szolga* azonosítóját), küld egy nyugtát az adott címkének viszont, ha egy időben több mint egy címke válaszol az azonosítójával, vagy csak részlegesen ütköznek keretek, azok eldobásra kerülnek.

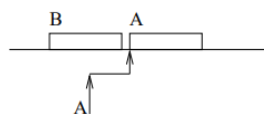


16. ábra: réselt ALOHA adatkeretek ütközése (t : ütközés által kiesett idő)
(Gábor, 2008)

Ha nem kapott nyugtát az adott címke akkor valamennyi idő múlva újra próbálkozik és elküldi az azonosítóját, ameddig el nem fogy a maximálisan felprogramozott próbálkozási lehetőség vagy nyugtát nem kap. A protokoll előírása szerint azonos kerethosszakokat kell használni.

Miután az olvasó összegyűjtötte a közelében lévő összes „tag” azonosítóját, kiválaszt egyet, majd várja a kártyától a SAK (Select AcKnowledge – kiválasztás tudomásul véve) üzenetet majd folytatja az azonosítást és egyéb memória műveleteket, addig a többi visszalép készenléti állapotba és vár további utasításra.

Több aktív eszköz jelenlétében is szükség van közeghozzáférési protokollra, ebben az esetben CSMA-t (Carrier Sense Multiple Access – vívőérzékeléses többszörös hozzáférés) alkalmaznak.



17. ábra CSMA illusztráció (Gábor, 2008)

Mielőtt „A” olvasó jelet adna, belehallgat a csatornába, ha foglalt akkor addig vár ameddig „B” befejezi az aktuális feladatát, majd amint végzett „A” azonnal elkezdi a beolvasást.

4. Széchenyi István Egyetem beléptetőrendszerének tesztelése

A dolgozatíráshoz az ihletet a Széchenyi István Egyetemen üzemelő kártyás beléptető rendszer szolgáltatotta, különböző okok miatt szükség volt több példányra egy kártyából, ez további motivációt szolgáltatott egy kisebb kutatásra majd annak kiteljesítésére.

4.1 tag-ek (címkék) adatvédelme, sokszorosíthatósága

Az említett helyszínen alkalmazott rendszer kártyái alapvetően rendelkeznek titkosítással, viszont nincs alkalmazva, mégpedig egy viszonylag érdekes rés nyomán. Specifikáció szerint (NXP, 2017), összesen 1kB-nyi tárhely áll rendelkezésre, ez 16 szektorra van elosztva, a nulladik szektor nulladik sora (18.ábra: piros egységek) tartalmazza az egyedi gyártási azonosítót (UID-t – Unique IDentificator-t, ami alapesetben ROM - **Read Only Memory**, csak olvasható memória). Mindegyik egység tartalmaz négy blokkot (későbbiekben sort) amik egyenként 16 bájtosak, az adatmezők mindegyike hexadecimális (0-tól, F-ig) értékek formájában tárol adatokat és egyenként két kulccsal rendelkezik (18.ábra: zöld és narancs egységek), így akár mind a 16 szektornak megadható 1-1 egyedi kulcspár (18.ábra).

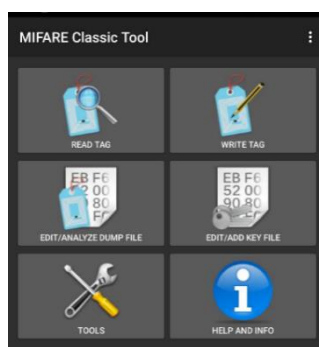
MiFare 1K, 720 usable bytes

Sector #0	Block #0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Block #1	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Block #2	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
	Block #3	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Sector #1	Block #4	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
	Block #5	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
	Block #6	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
	Block #7	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
Sector #2	Block #8	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143
	Block #9	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
	Block #10	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175
	Block #11	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
...																	
Sector #15	Block #60	960	961	962	963	964	965	966	967	968	969	970	971	972	973	974	975
	Block #61	976	977	978	979	980	981	982	983	984	985	986	987	988	989	990	991
	Block #62	992	993	994	995	996	997	998	999	1000	1001	1002	1003	1004	1005	1006	1007
	Block #63	1008	1009	1010	1011	1012	1013	1014	1015	1016	1017	1018	1019	1020	1021	1022	1023

18. ábra szektorok adatstruktúrája (Rose, 2021)

A fehérrel jelzett mezőknek nincsen különleges funkciójuk, adattárolásra alkalmasak. Minden szektor utolsó sora tartalmazza: A (zöld) kulcsot, lilákban a hozzáférési feltételeket, majd szürkével egy „szabad” bájtot és B (naranccs) kulcsot (ha B kulcsra nincs szükség a bájtjai konfigurálhatóak adatmezőként is).

Androidos rendszerre elérhető a gyártó (Mifare) hivatalos alkalmazása (19.ábra), ami a Classic kártyacsalád tagjaival képes műveleteket végrehajtani. (lényeges funkciók: írás, olvasás, adatmezők szerkesztése, klónozás).

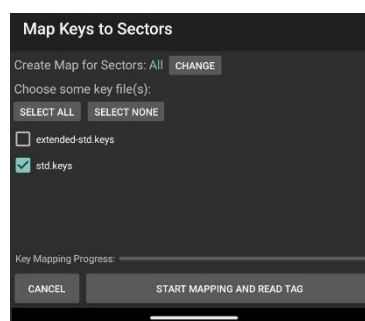


19. ábra Mifare Classic tool

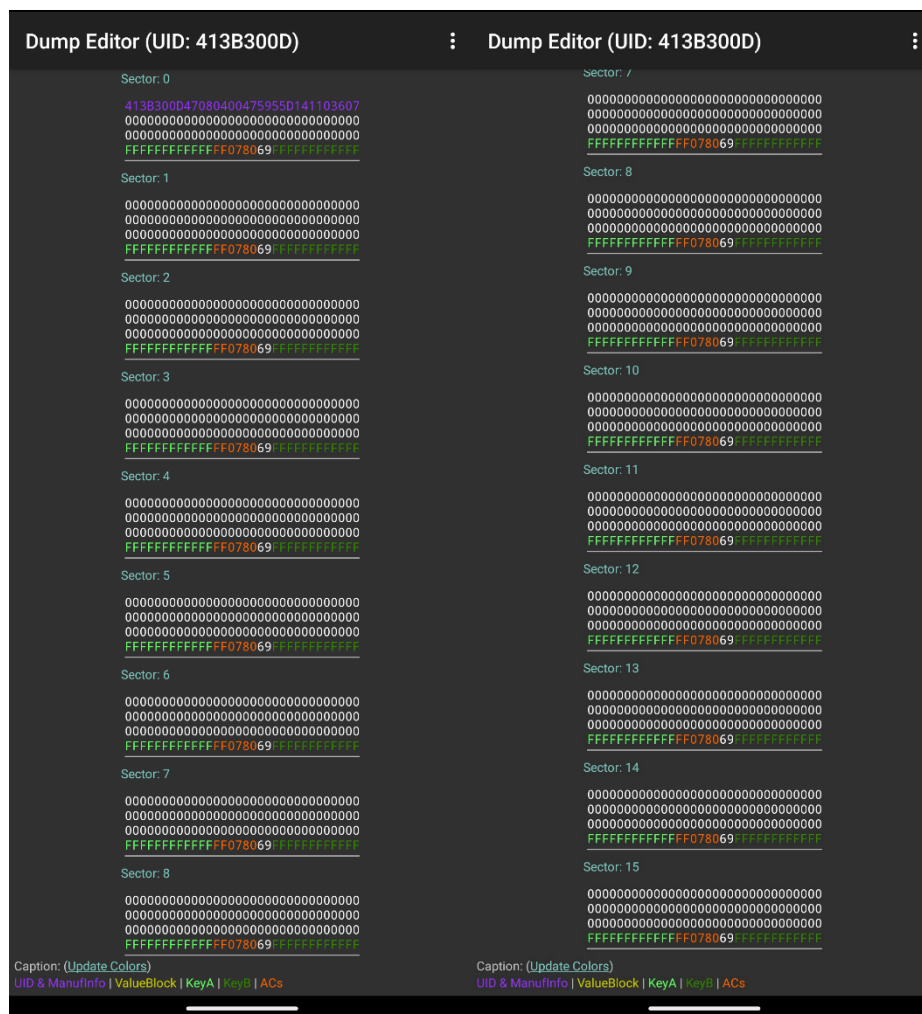
Klónozás céljából extra címkékhez nem nehéz hozzájutni, internetes áruházakon keresztül könnyen beszerezhetőek, még ha formára több félével is lehet találkozni (kulcstartó, kártya, korong, matrica stb.) igazából kettőt különböztetünk meg. Az eredeti és második

generációs (2nd gen magic tag) „varázs címkéket”, az eltérés a két kiadás között parányi mégis döntő súllyal bír. A „magic tag”-ek azzal a speciális tulajdonsággal bírnak, hogy írható a nulladik blokk első sora, ami az egyedi azonosítót tartalmazza, így ez nélkülözhetetlen a kísérlet szempontjából.

Az első próbálkozások alkalmával semmi különös információ nem került feltárára, az eredeti kártya gond nélkül beolvashatónak bizonyult, ebből következett, hogy a kulcs mezők és a hozzáférési kondíciók is az alapértelmezett értékekre vannak beállítva (21.ábra, zöld kulcs karakterek és narancssárga hozzáférési kondíciók). A címke olvasás menüpontban elegendő kiválasztani az „std.keys” (standard kulcs) fájlt (20.ábra), ami tartalmaz három lehetséges kulcsot, FFFFFFFFFFFFFFFF, A0A1A2A3A4A5, D3F7D3F7D3F7. Ha van egyedi kulccsal ellátott címkénk akkor szükségessé válik betölteni vagy a kulcs(ok) birtokában kézzel írni egy kulcs fájlt. A start gomb megnyomása után elindul az olvasási folyamat és pár másodperc után minden tárolt adat láthatóvá válik. Az eredeti kártya is megegyező eredményeket produkált, annyi eltéréssel, hogy más azonosítót foglalt magában az első sor. Az adathalmazokat összehasonlítva egyértelművé vált, hogy ebben az esetben elegendő az egyedi azonosítót átmásolni egy üres címkére.



20. ábra Kulcs fájlok



21.. ábra véletlenszerű kártyáról beolvasott szektorok

A másolási procedúra a következőképpen zajlik:

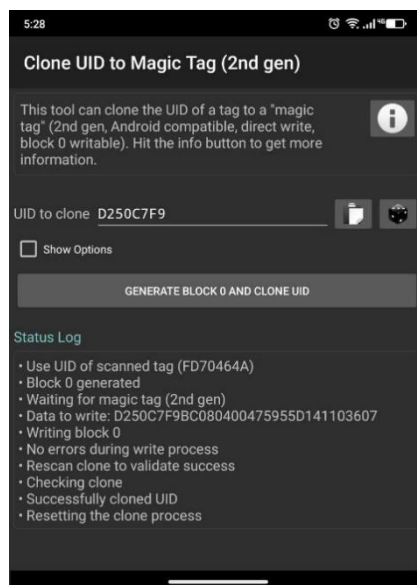
-*Write tag* menüpontban *Clone UID*-t kell kiválasztani.

-A telefon hátuljához tartva a másolandó kártyát, a klónozó program beolvassa az UID-t a másolandó azonosító helyére (22.ábra, *D250C7F9*).

-Majd a 0.szektor első sorának létrehozása a *generate block0 and clone UID* gombbal.

-A program kéri a felülírandó címkét (22.ábra, *FD70464A*), amint érzékeli elkezd a klónozási folyamatot, átírja a 0.szektor első sorát.

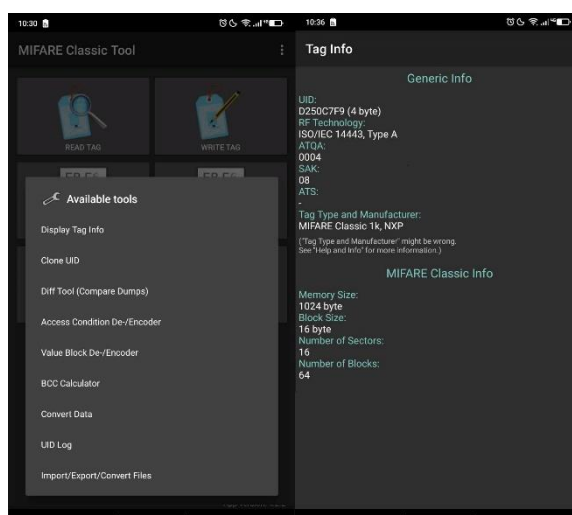
-Miután végzett megerősítést kér egy újra olvasással és nyugtázza a műveletet amennyiben az sikeres.



22. ábra Klónozási folyamat

4.2 Hallgatózás

Az ISO 14443-as (RFID kommunikációs) szabványból kétfélét különböztetünk meg: A és B típusút. A mérések megkezdése előtt fontos eldönteni, hogy melyik fajtát kell beazonosítani (ehhez nagy segítséget fog nyújtani a fentebb taglalt alkalmazás), majd ebből kikövetkeztethető a rádiós jeleket demoduláló kapcsolás felépítése. A *Tools* menüpontban (19.ábra) megtalálható *Display Tag Info* eszközre (23.ábra) lesz szükség. A kártya beolvasása után az általános információk alatt megtalálható a keresett rádiós szabvány (A) típusa.



23. ábra: kommunikációs szabvány feltárása

Szabvány	Típus	Írány	Moduláció	Kódolás	Segédvívő	Adatátvitel sebessége
14443	A	adó→vevő vevő→adó	ASK 100% ASK 10%	Miller Manchester	nincs 847.5kHz	160kbps
	B	adó→vevő vevő→adó	ASK 10% BPSK	NRZ	nincs 847.5kHz	

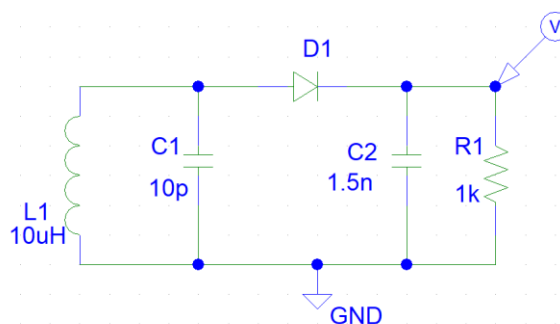
2. táblázat: ISO/IEC 14443 A/B RFID szabvány 13.56MHz-en

A táblázat szerint az *A* szabvány esetében, ASK-el modulált jeleket kell keresni. Az adó→vevő irányú kommunikáció esetében 100%-os modulációs szintű képre lehet majd számítani, mint például a 15.ábra felülről harmadik függvénye. Logikai egy esetén az oszcillátor amplitúdója nem csökken viszont, amikor *nulla* következik az alapjel teljesen megszűnik a 100-100 = 0%-os jelszint miatt.

Vevő→adó irányban a 10%-os szint azt jelenti, hogy az alapjel amplitúdójának 100-10 = 90%-ára kell számítani amikor logikai egy-el modulált feszültség szint után *nullával* moduláltat keresünk.

A kísérletek folyamán sokféle lehallgató kapcsolás és annál is több oszcilloszkóp beállítás kipróbálása árán sikerült elérni egyértelműen beazonosítható jelalakokat. A kezdeti szakaszokban a lehető legegyszerűbb módszerrel, egy alacsony (100 μ H) induktivitású vasmagos tekercset antennaként használva, mindenféle kapcsolás nélkül történtek a próbálkozások. Ezzel a módszerrel sok eredményt nem lehetett elérni, a zajos, „triggerelhetetlen” jeleken és a felismerésen kívül hogy ez önmagában kevés lesz.

Hosszas adatlapok, rádiós könyvek és egyéb kísérletek böngészése után azt a konklúziót lehetett levonni hogy az eredetileg a címkékben alkalmazott AM rádiós detektoros (angolról fordítva envelope detector: „boríték fogó”) kapcsolás (7.ábra) a néhány módosítással tökéletes lesz erre a célra. A modulátor MOSFET elhagyásával és a címke mikrovezérlőjének helyére egy oszcilloszkópot csatlakoztatva (24.ábra) sikerült eredményesen mérni. Az alábbi (24.) ábrán a kísérletben használt pontos értékek vannak feltüntetve.



24. ábra: „borítékfogó kapcsolás”

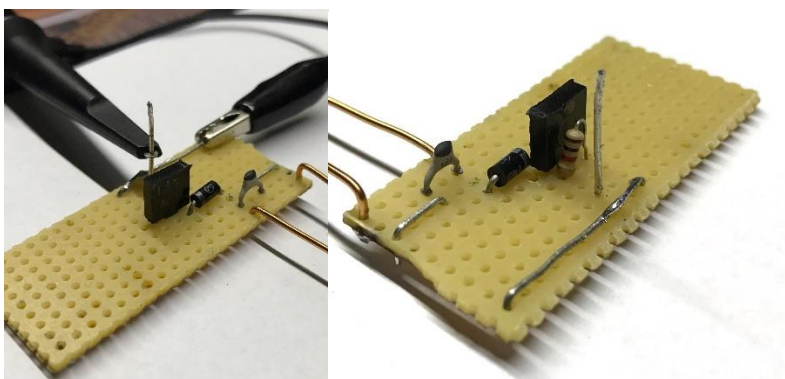
A kapcsolás működési elve: L1 az antenna tekercs és C1 kondenzátor párhuzamos hangolt rezgőkört alkot, ami a jobb vétel érdekében az üzemi frekvencia 13.54 MHz környékére lett hangolva, a fentebb említett Thomson képlet szerint $f_0 = 15.91$ MHz-re. Bár a hallgatózási eredményeket az eltérés szignifikánsan nem befolyásolta, az oka említésre méltó. Abból adódik,

hogy a szabványos alkatrész (tekercs és kondenzátor) érték párokból nehéz pontosan behangolni egy áramkört (ez a probléma kiküszöbölhető egyedi alkatrész készítésével).

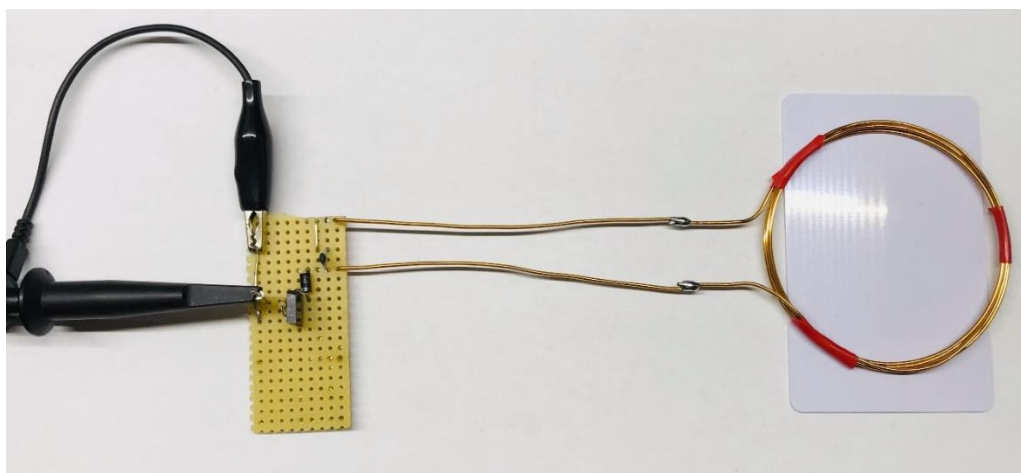
A D1-es dióda leszűri a váltakozó áramú komponenseket majd C2 és R1 aluláteresztő szűrőt alkotva jelentősen lecsökkenti a vivőfrekvencia hatását a V mérési ponton, így láthatóvá válik az eredeti jelalak.

Kivitelezéskor elő fordult még egy probléma: az antennaként használt tekercs nem lehetett a „borítékfogó” kapcsolás közelében a nagy térerő miatt. Az olvasó tekercsének erős sugárzása áramot képes indukálni az áramkör többi alkatrészében, azok kivezetésein, és a prototípus panel vezetősávjain. Ez a jelenség olyan mértékben befolyásolta a méréseket, mintha nem is működne a kapcsolás. Megoldásként 10cm-el meghosszabbításra kerültek az antenna kivezetései.

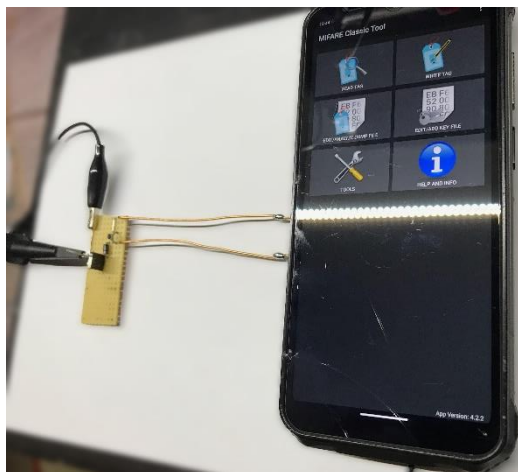
Mérési összeállításról készült képek:



25. ábra: „borítékfogó kapcsolás” prototípus panelon megvalósítva

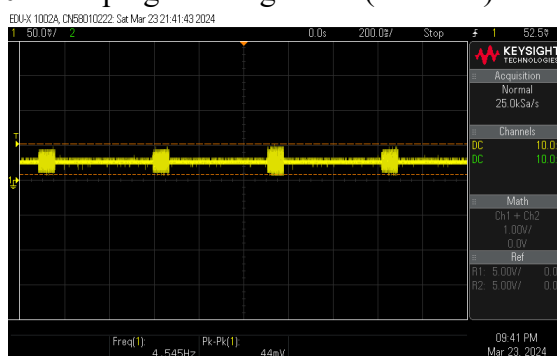


26. ábra: „borítékfogó” kapcsolás mérési összeállítása beléptetőkártyával



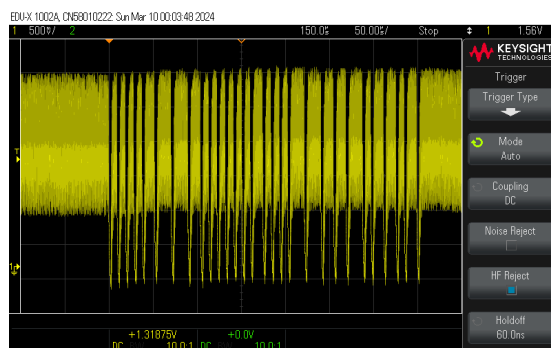
27. ábra: „borítékfogó” kapcsolás olvasóként okostelefont alkalmazva

A mérések során több különböző érdekes jelenség volt megfigyelhető. Egy „tag” általában már 4cm-ről olvasható. Amikor ezen a távolságon kívül, de maximum 10cm-en belül merőlegesen közelített a telefon tekercsére egy kártya, akkor már az olvasó elkezdett kb. 500ms-os periódus idővel 40ms-os ping-eket sugározni (1. mérés).



28. ábra: periodikus ping-ek

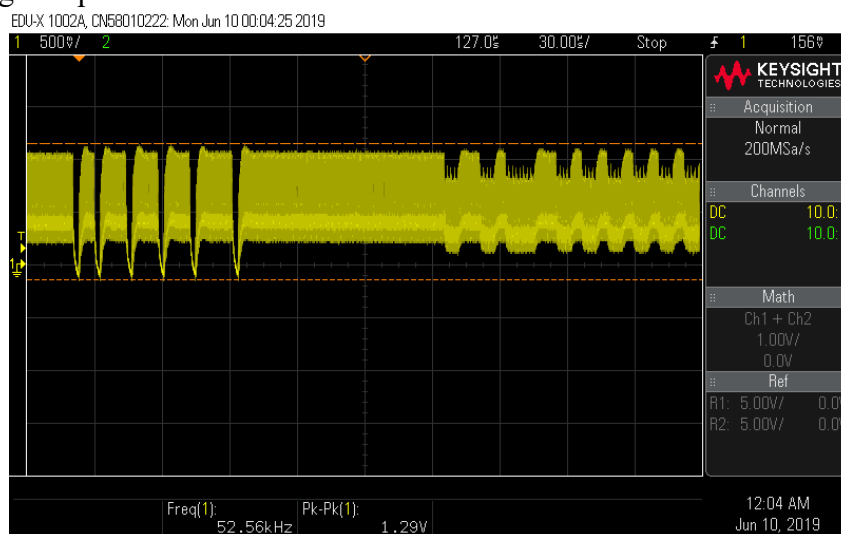
Az első mérések folyamán a jelek tulajdonságainak megismerése folyt. Az első eredményes triggerelés a jelszint közepére állítva fogott jelet a nagyfrekvenciás komponensek figyelmen kívül hagyásával (29. ábra, HF reject). A demodulált digitális jel nagy kitéréseiből



29. ábra: első elfogott jel

arra lehet következtetni, hogy a fentebb említett 100%-os modulációs szintű jel látható, ami az olvasó → kártya irányú adatfolyamot tartalmazza. A 29. ábra alapján világossá vált, hogy a zajos

átlagjel alá és a 0-feszültség közé érdemes beállítani a triggerelési szintet, megcélózva a lefelé mutató tüskéket. Az előbbi megállapításokat alkalmazva a 30.ábrán nagyon szép jelalakot sikerült lencsevégre kapni.



30.ábra: helyes triggerelési szint beállítva

A 29.ábrához képest sokkal rövidebb lefelé irányuló kommunikáció után láthatóvá váltak a címke által visszaküldött bitek, a csekély feszültség ingadozás arra mutat, hogy valóban 10% körüli modulációval dolgozik a szabvány. Nagyobb időalapot és más jelformálási módszert (acquisition-t) választva (Normal helyett High Res-t – nagy felbontást) egy teljes, illetve több egész üzenetet is lehetséges sokkal jobb olvashatósággal elfogni (31.ábra). Fontos megjegyezni, mivel ritka események elfogása a cél, érdemes a digitális tárolós oszcilloszkópok

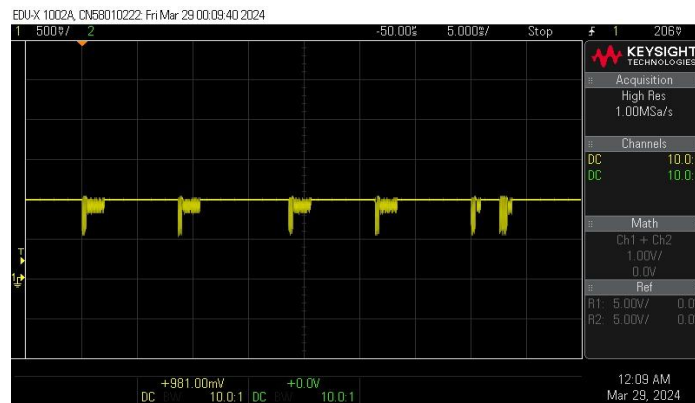


31.ábra: teljes újrárás végi, egész, oda-vissza adatcsomag

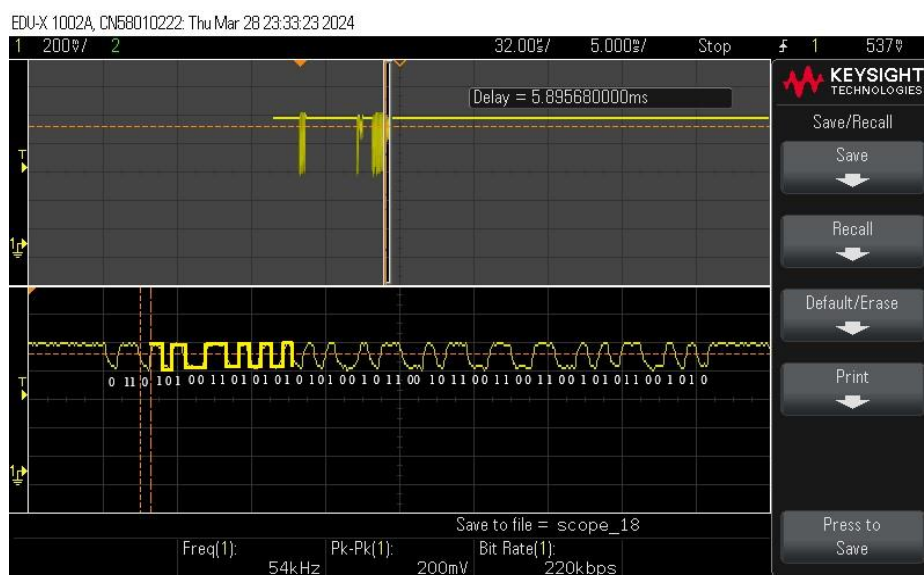
Single (egyszeri) mintavételezési módját alkalmazni, mivel a keresett jel nem periodikusan ismétlődő és szükség van minél nagyobb felbontásra a kiértékeléshez. *Single* üzemmódban egyetlen „képet” készít és tárol az oszcilloszkóp így a teljes memóriát ki lehet használni. A jelről ez által kétszer nagyobb felbontású kép kapható a folyamatosan mintavételező automata módhoz képest, ahol egyszer mintavételezi, másodszor kirajzolja az előzőleg vett jelet az

oszilloszkóp. A két művelet szimultán végrehajtásához (egyszerre vagy írni, vagy olvasni lehet egy memóriába), két adattárolóegységre van szükség, így ebben az esetben kettéosztva üzemel a memória.

A 31.ábrán egy kártya teljes újraírása során elfogott utolsó adatsomag látható. A művelet közben az egyedi csomagokban jellemzően hosszabb ideig tart az olvasó kommunikációja a címke irányába, mint visszafelé (32.ábra).

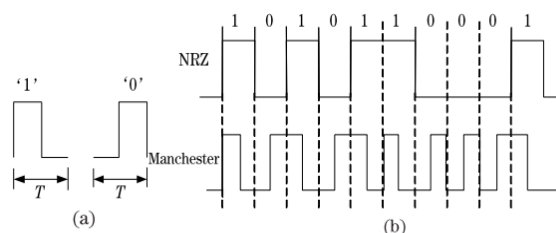


32.ábra: teljes kiolvasás közben elfogott adatsomagok



33.ábra: címke->olvasó, kommunikáció manuális kiértékelése dekódolás nélkül

A 2.táblázatból tudjuk, hogy a visszafelé kommunikáció *Manchester* kódolást használ, ami a következőképp működik: a 0-biteket az $1 \rightarrow 0$ átmenet, az 1-biteket pedig a $0 \rightarrow 1$ átmenet

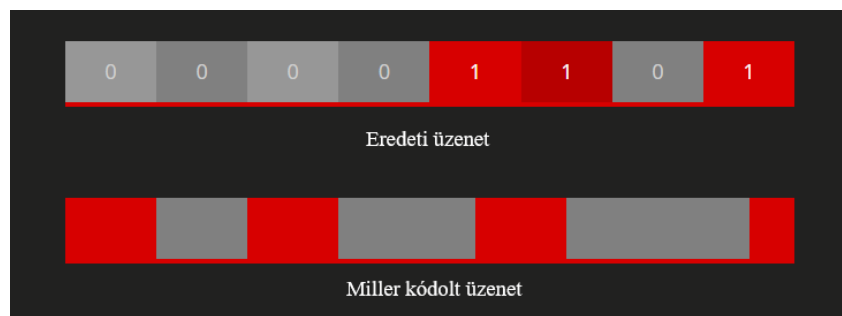


34. ábra: Manchester kódolás (Zhou, 2010)

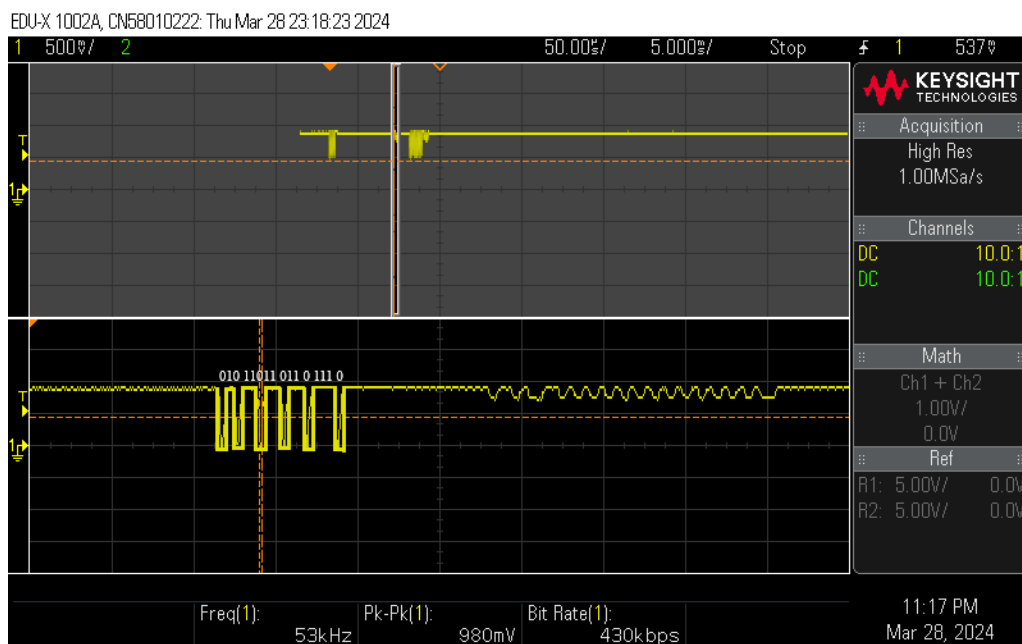
szimbolizálja (34/a, ábra). Ha több egyforma bit következik egymás után akkor a jel félidőben visszatér az előző állapotba így a következő bitet szintén jelváltás fogja szimbolizálni (34/b, ábra utolsó 3db nullás sorozat), ezzel megakadályozható az adatfolyam kezdetén jelentkező bizonytalanság az első bit mivolta tekintetében, és a szinkronvesztés. 34.ábra szerinti példa dekódolás: az első 2 váltás (33.ábra, első négy bitje, 0110) dekódolt megfelelője egy 0 majd azt követően logikai 1- értéket takar.

Lefelé kommunikáció esetében *Miller* kódolást (34.ábra) használ a szabvány. Elvét tekintve három szabályt alapján kódolható az alapjel:

- Ha a jelenlegi bit 0, akkor **nem invertálja** a jelet.
- Ha a jelenlegi bit 0 és az előző is az volt akkor **invertálja** a jelet a bit „élénél”.
- Ha a jelenlegi bit 1, előző 0 vagy 1, akkor **invertálja** a jelet a bit közepénél.



34.ábra: Miller kódolás



35.ábra: olvasó->címke kommunikáció manuális kiértékelése dekódolás nélkül

A 35. ábrán invertált Miller kódolt jel látható 0101 1011 0110 1110 bináris értékekkel, dekódolás után a következő biteket adják vissza: 0000 1001 1001 1101. Manchesterhez képest az az előnye, hogy kisebb sáv szélességet használ, és ellenállóbb az interferenciát képző zajokkal szemben. Hátránya a bonyolultabb megvalósítás.

5. Javaslatok a javításra

Megelőző intézkedésként érdemes használatba venni a jelenleg is elérhető titkosítási funkciókat (A és B kulcsokat), a nagyobb biztonságot igénylő helyiségek belépési feltétele kiegészíthető biometrikus azonosítással, fontolóra vehető a magasabb biztonságú, korszerűbb titkosítási metódusokat használó rendszer telepítése.

Jövőbeli tervek

Szeretném tovább vinni a kutatást, célom a jelenlegi tudásszintemet fejlesztve, jobban megismerni különböző támadási módszereket, *open source* (nyílt forrású) kártyaolvasókkal kísérletezni, később biztonsági rendszerek fejlesztésében, kialakításában részt venni.

Konklúzió

A kutatás során ismertetésre került az RFID rendszerek működési elve szükséges részletekig, fény derült egy súlyos biztonsági kockázatra az egyetemen használt kártyás beléptető rendszerben, kísérletek folytak a két fél közti kommunikáció lehallgatására.

Irodalom

- Dobkin, D. M. (2007). *The RF in RFID*. Newness.
- EMVCo, L. (2024). *EMVCo*. Forrás: <https://www.emvco.com/emv-technologies/>
- Finkenzeller, K. (2010). *RFID Handbook*. Wiley.
- Frederic Le Roy, Ali Mansour, R. Lababidi, & Denis Le Jeune. (2016. szeptember). *research gate*.
Forrás:
https://www.researchgate.net/publication/321058198_RFID_Eavesdropping_Using_SDR_Platforms
- Gábor, L. (2008). Aloha protokoll. In L. Gábor, *Számítógépes hálózatok* (old.: 14). Győr: Universitas Győr Nonprofit Kft.
- Hamed Rahmani, A. B. (2020. Augusztus). *An Integrated Battery-Less Wirelessly Powered RFID Tag with Clock Recovery and Data Transmitter for UWB Localization*. Forrás:
<https://ieeexplore.ieee.org/document/9223821>: <https://www.semanticscholar.org/paper/An-Integrated-Battery-Less-Wirelessly-Powered-RFID-Rahmani-Babakhani/3a478d91df9ea771d538e9c3c7ef11f05a00efa0>
- Herdx. (2024). Forrás: <https://herdx.com/rfid-cattle-tags/>
- Maulana, F. (2021). *IEEE Xplore*. Forrás: ieeexplore.ieee.org:
<https://doi.org/10.1109/ICCSAI53272.2021.9609762>
- Mulliner, C. (2011. Június 18). *mulliner.org*. Forrás: Berlin Institute of technology:
http://mulliner.org/nfc/feed/nfc_ndef_security_ninjacon_2011.pdf
- NXP. (2017. November 23). *NXP semiconductors*. Forrás: https://www.nxp.com/docs/en/data-sheet/MF1S50YYX_V1.pdf
- OpenUniversity. (2024). *Open learn*. Forrás: <https://www.open.edu/openlearn/digital-computing/exploring-communications-technology/content-section-1.4>
- P. Nikitin, S. R. (2013). *Semantic Scholar*. Forrás: <https://www.semanticscholar.org/paper/Simple-Low-Cost-UHF-RFID-Reader-Nikitin-Ramamurthy/4f1c815c7e4e20270a29e72779dbca0403b11a52>
- Pál, T. Á. (2021. Január 8). *Portfolio*. Forrás: portfolio.hu:
<https://www.portfolio.hu/bank/20210108/hiaba-lelt-kotelezo-nem-minden-boltban-fizethetunk-keszpenzmentesen-magyarorszagon-464380>
- Roberti, M. (2005). *RFID Journal*. Forrás: The History of RFID Technology:
<https://www.rfidjournal.com/the-history-of-rfid-technology>
- Rose, G. (2021. november 26). *Medium*. Forrás: <https://grave-rose.medium.com/mifare-1k-classic-dd561424a41b>
- Sony. (2021. 01 26). *www.sony.com*. Forrás: <https://www.sony.ie/electronics/support/articles/00256824>
- Staff. (2014). *RFID Journal*. Forrás: <https://www.rfidjournal.com/question/how-do-i-deactivate-an-rfid-tag>
- Zhou, R. (2010. május). *Research Gate*. Forrás: https://www.researchgate.net/figure/a-Manchester-coding-b-Manchester-and-NRZ_fig1_250000193