



FAKULTETA ZA RAČUNALNIŠTVO IN
INFORMATIKO IN FAKULTETA ZA
MATEMATIKO IN FIZIKO

PROJEKT PRI PREDMETU KRIPTOGRAFIJA IN
TEORIJA KODIRANJA 2

Identifikacija z RFID oznakami s pomočjo kriptografije

Avtor:
Slavko ŽITNIK

Mentor:
prof. dr. Aleksandar
JURIŠIĆ

5. december 2010

KAZALO	1
--------	---

Kazalo

1. Uvod	2
2. Opis RFID oznake	2
2.1. Tipi RFID oznak	2
2.2. RFID in pametne brezkontaktne kartice	3
2.3. Primeri uporabe	5
3. Napadi na RFID čipe	5
3.1. Napadi na fizičnem nivoju	5
3.1.1. Trajno uničenje čipa	5
3.1.2. Začasna onesposobitev čipa	6
4. UMAP Protokoli	7
4.1. SASI protokol	7
5. Zaključek in ugotovitve	8

1. Uvod

Tehnologija RFID (*Radio Frequency IDentification*) nam omogoča identifikacijo preko radijskih valov. V zadnjih letih postaja zaradi vse nižje cene vse bolj popularna pri množični uporabi označevanja, sledenja predmetov. V prihodnosti se pričakuje, da bo popolnoma nadomestila identifikacijo s črtnimi kodami. Zaradi tega v tej seminarski opisujemo dva protokola, ki se lahko uporabljata v cenениh RFID oznakah.

Poleg svoje vsestranske uporabe pa se pojavljajo tudi varnostni problemi. Napadi lahko prihajajo od kogarkoli, tudi iz oddaljenosti več 10 metrov. V potrošniški uporabi je ena glavnih potreb zagotavljanje anonimnosti oziroma onemogočanje sledenja (*tracking*) Velikemu bratu. Prav tako je velik problem tudi, če bi o nas lahko kdo izdelal osebni profil (*profiling*) in nas nato identificiral glede na množico označenih predmetov (*hotlisting*).

V gospodarstvu pa želimo z novimi tehnologijami poceniti, pohitriti delovanje z enako varnostjo in nizkimi stroški vložka. Oznake želimo imeti čimcenejše in čimmanjše. Vsak RFID vsebuje mikročip, na katerem se lahko izvajajo računske operacije. Po občutku se cena oznake za vsakih dodanih 1000 logičnih vrat v čipu, poveča za 1 cent. Cilj te seminarske naloge je, da predstavimo protokola, ki nista računsko kompleksna, a vseeno omogočata varno identifikacijo.

Za nekatere storitve nekaj EUR za izdelavo RFID oznake ne predstavlja velikega stroška, saj jo lahko večkrat uporabljamo in si posledično lahko privoščimo boljše zaščito. To pa ne pomeni, da pri masovni uporabi v knjižnicah, skladiščih ne potrebujemo varnosti.

2. Opis RFID oznake

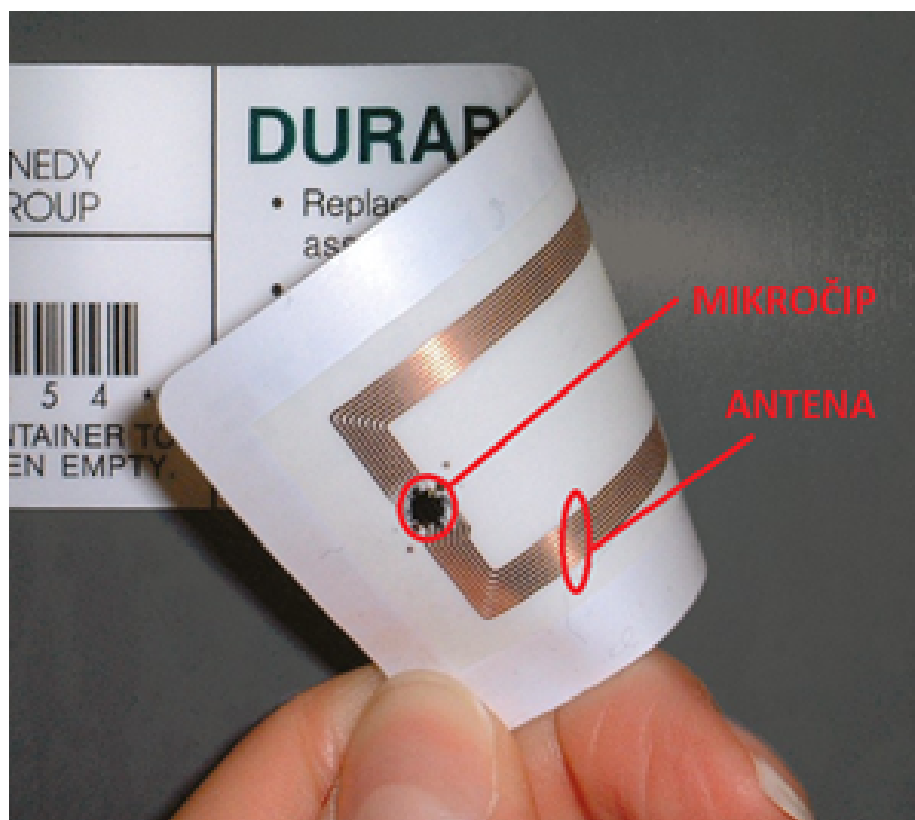
RFID je majhno elektronsko vezje, ki ga v sistemu imenujemo oddajnik ali oznaka. Sestavljen je iz integriranega vezja (čipa), ki hrani in procesira podatke, ter izvaja modulacijo in demodulacijo signalov. Drugi del oddajnika je antena, ki sprejema in oddaja radijske signale. Signale RFID oddajnikov sprejema RFID čitalec, kar nam omogoča identifikacijo predmetov oziroma bitij.

Na sliki 1 si lahko ogledate tipično sestavo RFID oznake.

2.1. Tipi RFID oznak

RFID sisteme delimo glede na napajanje (aktivni/pasivni) in način prenosa podatkov (induktivni/elektromagnetni). Več o tem si lahko preberete tudi na Wikipediji:

- Tip napajanja:
 - *Aktivni RFID*: Oddajniki vsebujejo lastno napajanje (majhno baterijo). Zaradi tega se oznaki poveča cena, a imamo zaradi tega daljši domet in bolj zanesljivo delovanje v šumnih okoljih.
 - *Pasivni RFID*: Oddajniki ne vsebujejo lastnega napajanja, ampak potrebno energijo pridobijo iz induciranja signala v anteni. S tem se signal dovede do čipa, ki se "zbudi" in prične z delovanjem. Ker oddajniki nimajo baterije, so zato zelo poceni, a imajo krajši domet, a tudi manj nezanesljivo delovanje.

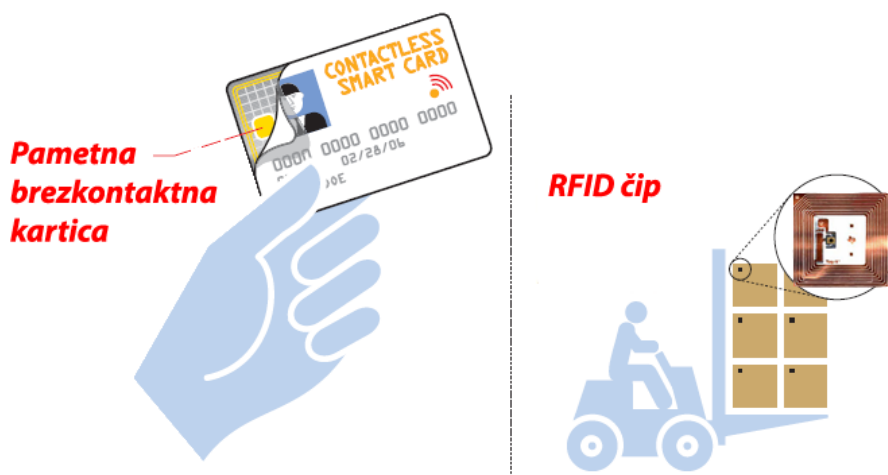


Slika 1: Prikaz RFID oznake

- Način prenosa podatkov:
 - *Induktivni RFID*: Oddajnik za prenos informacije uporablja princip magnetne indukcije. Preko dveh tuljav, ki sta priklopljeni na čip inducira napetost. Komunikacija s čitalcem deluje v bližnjem polju, zato je doomet do nekaj 10cm. Oddajnik informacijo prenese čitalcu prek uporabe bremenske modulacije, ki pomeni spreminjanje sklop-nega faktorja v odvisnosti od poslanih podatkov.
 - *Elektromagnetni RFID*: Oddajnik komunicira preko elektromagnetnih valov, ki jih oznaki pošilja čitalec in se le ti odbijajo od oddajnika. Ta odboj se izkoristi, da se prenese informacija od oddajnika do čitalca. Ko se čip zbudi, začne spreminjati frekvenco signala glede na podatke, ki jih pošilja - modulacijski odboj.

2.2. RFID in pametne brezkontaktne kartice

Brezkontaktne pametne kartice (V svoji seminarski nalogi jih opisuje Moškon) je pametna kartica, ki lahko preko radijskih valov komunicira z oddaljenim terminalom. Značilno sta čip in antena zapakirana v plastičnem ohišju velikosti bančne kartice. Glavna lastnost, ki jo loči od cenejših RFID čipov je večji spomin in možnost izvajanja internih kriptografskih operacij. Zaradi tega



Slika 2: Prikaz razlike med pametno brezkontaktno kartico in RFID čipom

omogoča večjo varnost in uporabo znanih kriptografskih pokolov. Ker je od RFID čipov večja in predvsem dražja, jo je neekonomsko uporabljati množično v skladiščih, trgovinah,... Kratko primerjavo značilnosti obeh si lahko ogledate v tabeli 1. V praksi za pametne kartice pogosto uporabljamo kar ime RFID

	Pametna brezkontaktna kartica	RFID čip
Cena	0,5EUR ali več	manj od 0,05EUR
Fizična velikost	od 25x15mm debeline 1mm	od 5x5mm debeline papirja
Zmogljivost procesorja	možnost izvajanja kriptografskih funkcij	osnovne matematične operacije
Velikost pomnilnika	več KB	do 2Kb
Delovna razdalja	do 15cm	do nekaj 10m
Varnost podatkov	lahko zelo dobra	slabša

Tabela 1: Primerjava pametne brezkontaktno kartice in RFID čipa. Cene so bile pridobljene v spletni trgovini podjetja *1 Klik d.o.o.*

čipi, zato si pogledajmo naslednjo delitev, da se bomo še lažje odločili.

- Dražje (*High cost*) oznake: Te lahko obravnavamo kot pametne brezkontaktno kartice in so tudi dovolj zmogljive za uporabo javne kriptografije.
 - "Polno-kvalificirane" (*Full-fledged*): Imajo notranjo zmogljivost izvajanja simetrične, javne kriptografije, računanja enosmernih kriptografskih funkcij,...
 - "Enostavne" (*Simple*): Imajo zmožnost računanja naključnih števil in računanja zgoščevalnih funkcij.
- Cenejše (*Low cost*) oznake: Te lahko obravnavamo kot RFID oznake.

- "Lahke" (*Lightweight*): Omogočajo operacije generiranja naključnih števil in enostavnih funkcij kot je računanje CRC napak, a ne izvajanja kriptografskih funkcij.
- "Ultralahke" (*Ultralightweight*): Omogoča računanje le osnovnih bitnih operacij XOR, OR, AND, ...

V nadaljevanju bomo prikazali dva pristopa, kako z ultralahkimi oznakami zagotoviti čimvečjo varnost. Svetovno najbolj razširjena standardizirana klasifikacija RFID oznak pa je EPCglobal (*Electronic Product Code*), ki na podoben način, kot smo mi zgoraj, razvrsti oznake v štiri razrede.

2.3. Primeri uporabe

RFID tehnologijo uporabljamo skoraj na vsakem koraku, a se tega sploh ne zavedamo. Najbolj se RFID sistemi uporabljajo v skladiščih. Oznake nam omogočajo enostavno sledenje izdelkov, optimalno poslovanje, evidenco zalog v vsakem trenutku. Veliko takšnih sistemov predvideva le označevanje palet, vendar nekatera globalna podjetja kot so Airbus, Boeing, Wal-Mart, označujejo tudi vsak izdelek posebej. RFID sisteme uporabljamo tudi v knjižnicah, mehaničnih delavnicah, bolnišnicah, trgovinah, v igralništvu, za pregled lastnega inventarja opreme, plačilo mestnega prometa (Urbana¹), beleženje delovnega časa, plačevanje cestnine (uporaba ABC v Sloveniji), ... RFID oznake bodo prisotne tudi v naših osebnih izkaznicah in potnih listih. Nekateri so hoteli tudi, da bi bil vsak evropski bankovec označen s svojo oznako.

Podjetje Nokia razvija tehnologijo NFC (*Near Field Communication*), ki bi združila to tehnologijo z mobilno in omogočila hitro in varno elektronsko poslovanje ali celo nadomestila uradni osebni dokument.

3. Napadi na RFID čipe

Raziskovalec Mitrokotsa s sodelavci so predlagali 4-nivojsko razdelitev napadov na RFID čipe [3], ki si jo lahko ogledamo na sliki 3. To je le ena izmed oblik klasifikacij, ki so jih predlagale tudi druge organizacije. Že na prvi pogled nam vzbudi podobnost s TCP/IP modelom. Predlagani nivoji si sledijo od fizičnega nivoja, do najvišjega strateškega, kjer lahko padejo prav vsi varnostni sistemi, saj je v neposredno v igro vključen tudi človeški faktor.

3.1. Napadi na fizičnem nivoju

Napadi na tem nivoju so povezani z naravo brezžičnega delovanja čipa in direktnega kontakta napadalca s čipom.

3.1.1. Trajno uničenje čipa

Odstranitev čipa. Ker so čipi ponavadi pritrjeni na izdelke kot nalepke, je zelo enostavno odstraniti čip in ga uničiti. Dražji izdelki, predvsem obleke v trgovinah, so označene s čipi tako, da potrebujemo posebne klešče, da lahko odstranimo čip.

¹Urbana je kartica za brezgotovinsko plačevanje mestnega potniškega prometa, parkirnin in ostalih storitev v Mestni občini Ljubljana, ki jo je le ta uvedla konec leta 2009.

Razmerje cena-uporabnost	Logistični faktorji	Omejitve okolja	Strateški nivo
CRM sistemi	ERP sistemi	Strežniška in vmesna programska oprema	Aplikacijski nivo
Sledenje ISO standardom	Sledenje EPC Gen standardom	Lastniški RFID protokoli	Omrežni/transportni nivo
Radijske frekvence	Strojna oprema čitalca	RFID oznaka	Fizični nivo

Slika 3: Razdelitev RFID tehnologije na nivoje, kjer lahko napadamo sistem

Uničenje čipa. Zaradi slabe zaščite lahko včasih čip uničimo tudi nenamerno, če z njim pretrdo ravnamo. Poleg tega so tudi slabo odporni na statično elektriko, ki tudi lahko povzroči njegovo nedelovanje.

KILL ukaz. Podjetji *Auto – IDcenter* in *EPCglobal* sta za RFID čipe predlagali ukaz *KILL*, ki bi za vedno onesposobil čip. Pravilo pravi, da naj bi vsak proizvajalec čipov določil unikatno geslo za vsak čip posebej, ki se ga uporabi ob klicu tega ukaza. Ukaz je bil razvit predvsem zaradi varnosti, saj takšno funkcionalnost potrebujejo trgovci, ki želijo ob prodaji izdelka zagotoviti, da pripadajočega čipa ne bi nihče več uporabljal dalje. Tu je bila predvsem na udaru zasebnost. Če si izberemo primer, da kupec kupi obleko in po nakupu RFID čip v obleki še vedno deluje, ga lahko trgovec enostavno spremlja, kar pa seveda ni sprejemljivo. Seveda pa lahko z namernim uničevanjem čipov tudi sabotiramo RFID sistem.

Zaščita

Proti takšnim napadom se tehnološko težko zaščitimo. Poskrbeti moramo predvsem za nadzor dostopa do izdelkov, varovanje prostorov. Če pa to ni izvedljivo, lahko čipe bolje pritrdimo ali jih celo vgradimo v izdelke, če je to mogoče. Proti napadu s *KILL* ukazom se lahko zaščitimo z učinkovitim upravljanjem gesel, saj standard predvideva 32-bitno geslo za izvedbo ukaza.

3.1.2. Začasna onesposobitev čipa

Napadalec lahko komprimira sistem tudi samo za določen čas. Kot vemo, se RFID skener in čip sporazumevata preko elektromagnetnega valovanja. To lastnost lahko izkoristimo tako, da kot napadalec čip prekrijemo z npr. aluminijasto folijo in tako ustvarimo Faradayevo kletko. Iz fizikalnih lastnosti sledi, da če imamo nek objekt v celoti obdan s kovino in hočemo z objektom komunicirati preko elektromagnetnega valovanja, to valovanje do objekta ne bo prišlo. (Več o tem pojavu si lahko preberete na Wikipediji [6]). Podobno kot zgoraj se lahko zgodi tudi, da nenamerno zaradi okoliščin (npr. ledu) začasno onemogočimo delovanje. Glede na namen onesposobitve čipov zato ločimo:

Pasivna interferenca. Do pasivne interference, prepletanja dveh ali več valovanj, lahko prihaja v okoljih s prekomernim elektromagnetnim šumom. Tega pojava ne štejemo med napade, saj se to dogaja nenameno. Močan šum v svoji okolici lahko povzročajo elektromotorji, radijski oddajniki,

električne napeljave... Zaradi takšnega okolja je moteno komuniciranje z RFID čipom.

Aktivno motenje. Aktivno motenje pa je napad s pomočjo zgoraj opisane pasivne interference. Cilj napada je, da napadalec ugotovi frekvenco, na kateri deluje RFID skener in nato namenoma moti komunikacijo z RFID čipi s svojim signalom.

Zaščita

Zunanje motenje lahko onemogočimo, če prostore, kjer želimo izvajati svojo dejavnost, obdamo z aluminijasto folijo. Na trgu pa obstajajo tudi posebne zidne barve in nalepke za okna, ki preprečujejo prehajanje sevanja. [odstranjeno...]

4. UMAP Protokoli

Leta 2006 je Peris-Lopez s sodelavci predstavil družino ultralahkih vzajemno-avtentikacijskih protokolov (UMAP - Ultralightweight Mutual Authentication Protocols), začenši z M²AP [4], ki so mu isto leto sledili še EMAP in LMAP.

Vsaka oznaka vsebuje ID število. Predlagani protokoli predvidevajo, da so oznake sposobne izvajanja le enostavnih bitnih operacij AND, OR, XOR, krožne rotacije v levo za y bitov in seštevanja po modulu 2^m .

Cilj tovrstnih protokolov je, da zagotavljajo varno avtentikacijo med računsko šibkim členom na eni strani in močnejšim na drugi strani. V ta okvir se lepo ugamejo RFID sistemi, saj želimo čimcenejše RFID oznake v sistemu. Poleg tega tudi zunanji prisluškovalci ne bi smeli ob komunikaciji vedeti, s katero oznako komuniciramo, če so prisluškovali tudi prej. Anonimnost oznake se zagotavlja s shranjenim psevdonimom, ki se sčasoma spreminja. Poleg tega morajo pri javni komunikaciji prikriti ID število, ki ga vsebuje oznaka.

4.1. SASI protokol

Hung-Yu Chien je leta 2007 predlagal protokol SASI (Strong Authentication Strong Integrity) za cenene RFID oznake, ki ga je predstavil v [2]. Varnostna analiza protokola pa je predstavljena v [5] in [1], ki jo bomo tudi mi opisali. Ker je bil eden prvih resnih protokolov v tem segmentu, si bomo v nadaljevanju pogledali njegovo delovanje.

Protokol predvideva, da imamo v sistemu RFID oznake, RFID čitalce in zaledni sistem s podatkovno bazo. Privzeto je, da je komunikacija med čitalcem in bazo varna. To lahko omogočimo z uporabo močnih kriptografskih algoritmov, saj so čitalec in strežniki računsko dovolj zmogljivi. Vsaka oznaka hrani ID številko in dva zapisa trojk (IDS, $K1$, $K2$). V zalednem sistemu je shranjena ID številka in zadnja posodobljena trojka. Prvi zapis trojke predstavlja stare vrednosti, drugi pa potencialne nove vrednosti, ki se bodo uporabile ob naslednji komunikaciji. Besede so dolge 96 bitov, oznaka pa mora imeti dovolj prostora, da shrani 7 takšnih besed (1 beseda za ID in po 3 za vsako trojko).

Protokol sestoji iz treh faz:

1. Faza identifikacije oznake
2. Faza vzajemne avtentikacije

3. Faza posodabljanja ključev

Potek protokola si lahko ogledate tudi v tabeli 2.

Čitalec	Oznaka
1. Faza identifikacije oznake $\xrightarrow{\text{hello}}$ $\xleftarrow{\text{IDS}}$	
2. Faza vzajemne avtentikacije $A = \text{IDS} \oplus K1 \oplus n1$ izbrisano ...	
3. Faza posodabljanja ključev $\text{IDS}_{\text{old}} = \text{IDS}$ izbrisano ...	

Tabela 2: Prikaz delovanja SASI protokola

1. Faza identifikacije oznake

Čitalec najprej nagovori oznako s sporočilom *hello*. Oznaka mu odgovori z naslednjim potencialnim IDS **psevdonomom**. Če ga čitalec ne najde v bazi, poskusi z nagovorom še enkrat in oznaka mu odgovori z IDS psevdonomom, ki je bil uporabljen nazadnje. Čitalec glede na posredovan psevdonom iz interne baze pridobi ID in ključa $K1$, $K2$.

2. Faza vzajemne avtentikacije

Čitalec zgenerira naključni števili $n1$ in $n2$ in s pomočjo njih izračuna števila A, B in C .

$$\begin{aligned}
 A &= \text{IDS} \oplus K1 \oplus n1 \\
 B &= (\text{IDS} \vee K2) + n2 \\
 \overline{K1} &= \text{Rot}(K1 \oplus n2, K1) \\
 \overline{K2} &= \text{Rot}(K2 \oplus n1, K2) \\
 C &= (K1 \oplus \overline{K2}) + (\overline{K1} \oplus K2)
 \end{aligned}
 \tag{1}$$

[izbrisano...] V enačbi 1 smo naredili osnovo za enačbo 2.

V nadaljevanju si bomo pogledali nekaj napadov in kako varen pred njimi je SASI protokol. [izbrisano...]

5. Zaključek in ugotovitve

Predstavili smo dva protokola, ki jih lahko uporabljamo za identifikacijo v RFID sistemih. V zadnjih letih RFID tehnologija počasi izpodriva starejše črtne kode in princip razvoja tovrstnih protokolov, ki delujejo na poceni oznakah, lahko pomaga le k večji uporabi, saj znižuje ceno celotnega sistema. V organizacijah, kjer bi morali označiti tudi več kot 10.000 izdelkov, veliko vlogo igra vsak stotin.

Ugotovili smo, da samo bitne operacije niso dovolj dobre, saj oblikujejo pričakovan rezultat. To težavo so najprej hoteli odpraviti s SASI protokolom, ki

pa ni bil povsem dobro premišljen, zato Gossamer uvaja še dodatno nebesedno funkcijo MixBits, ki javna sporočila naredi bolj randomizirana.

Vprašanje, ki se zastavlja, je: Ali se sploh lahko dobro zaščitimo? Obstaja več odgovorov, ki bi jih omejil na kriptografske protokole, računsko moč naprav in ljudi. Vsi trije faktorji so tudi v medsebojni odvisnosti. Če imamo na voljo veliko računske moči, lahko uporabimo najboljše kriptografske protokole, vendar to poveča ceno. Za RFID sisteme bi lahko za oznake uporabili kar brezkontaktno pametne kartice, ki so malo večje in bi rešili problem z varnostjo. Najti moramo dobro razmerje. Če imamo v sistemu veliko sodelujočih, ki jih ponavadi v RFID sistemih imamo, moramo vzeti v zakup tudi ta faktor. Lahko naredimo še tako varen sistem, a s trenutkom, ko ima nad njim popoln nadzor vsaj en človek, se ga da napasti preko njega.

Stvarno kazalo

Napadi, 5

Protokol, 7

SASI, 7

RFID, 2

aktivni, 2

elektromagnetni, 3

elektronsko vezje, 2

induktivni, 3

pasivni, 2

Literatura

- [1] T. Cao, E. Bertino, and H. Lei. Security analysis of the SASI protocol. *IEEE Transactions on Dependable and Secure Computing*, 2008, 73-77.
- [2] H.Y. Chien. SASI: A new ultralightweight RFID authentication protocol providing strong authentication and strong integrity. *IEEE Transactions on Dependable and Secure Computing*, 2007, 337-340.
- [3] A. Mitrokotsa, M.R. Rieback, and A.S. Tanenbaum. Classification of RFID attacks. *Gen*, 2009.
- [4] P. Peris-Lopez, J. Hernandez-Castro, J. Estevez-Tapiador, and A. Ribagorda. M 2 AP: A minimalist mutual-authentication protocol for low-cost RFID tags. *Ubiquitous Intelligence and Computing*, 2006, 912-923.
- [5] P. Peris-Lopez, J. Hernandez-Castro, J. Tapiador, and A. Ribagorda. Advances in Ultralightweight Cryptography for Low-Cost RFID Tags: Gosamer Protocol. *Information Security Applications*, pages 56-68, 2009.
- [6] Wikipedia. Faradayeva kletka,
[http : //sl.wikipedia.org/wiki/faradayeva_kletka](http://sl.wikipedia.org/wiki/faradayeva_kletka).