ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Semiaktivní RFID UHF TAG s generátorem náhodných čísel

Semi Active UHF RFID TAG with random number generator

Diplomová práce

Studijní program: Komunikace, multimédia a elektronika

Studijní obor: Sítě elektronických komunikací

Autor práce: **Bc. Petr Sviták**

Vedoucí práce: Ing. Bc. Lukáš Vojtěch, Ph.D.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Poděkování

Rád bych poděkoval vedoucímu diplomové práce Ing. Bc. Lukáši Vojtěchovi, Ph.D. a konzultantovi Ing. Bc. Marku Nerudovi, Ph.D. za jejich rady a čas, který mi věnovali při řešení dané problematiky.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Čestné prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze dne 21. května 2017 …….

Podpis

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Sviták** Jméno: **Petr** Osobní číslo: **406134**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra telekomunikační techniky**

Studijní program: **Komunikace, multimédia a elektronika**

Studijní obor: **Sítě elektronických komunikací**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Semiaktivní RFID UHF TAG s generátorem náhodných čísel

Název diplomové práce anglicky:

Semi Active UHF RFID TAG with random number generator

Pokyny pro vypracování:

Prostudujte problematiku realizace HW generátorů náhodných čísel použitelných pro nízkopříkonové aplikace. Navrhněte a zrealizujte semiaktivní RFID UHF TAG, obsahující generátor náhodných čísel a respektující standard GS1 EPC GEN2 tak, aby bylo řešení implementovatelné s využitím stávajících RFID UHF čipů. Řešení realizujte tak, aby generovaná náhodná (případně pseudonáhodná) čísla zaplňovala datový obsah uživatelské části paměti čipu a byla dále periodicky přepisována - obnovována, dle energetických možností napájení čipu. Řešení otestujte jednak v experimentu v RFID UHF systému, ale také pomocí vybraného testu na kvalitu použitých náhodných čísel.

Seznam doporučené literatury:

[1] Valentine, G.; Vojtech, L.; Neruda, M.: Design of Solar Harvested Semi Active RFID Transponder with Supercapacitor Storage. Advances in Electrical and Electronic Engineering; Ostrava13.4 (2015): p.344-349
[2] Vojtěch, L.; Kypus, L.; Kvarda, L.; Thiard, N.; Yannis, J.: Solar and wireless energy harvesting semi-active UHF RFID tag design and prototyping. Proceedings of the 16th International Conference on Mechatronics - Mechatronika 2014
[3] Dokumentace dostupná na https://www.random.org/ [on-line]
[4] Dokumentace Monza X-8K Dura RFID Chip dostupná na http://www.impinj.com/ [on-line]
[5] Dokumentace EM4324 dostupná na http://www.emmicroelectronic.com/ [on-line]

Jméno a pracoviště vedoucí(ho) diplomové práce:

Ing. Lukáš Vojtěch Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **17.02.2017** Termín odevzdání diplomové práce: **26.05.2017**

Platnost zadání diplomové práce: **30.09.2018**

Podpis vedoucí(ho) práce	Podpis vedoucí(ho) ústavu/katedry	Podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání	Podpis studenta

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Anotace:

Tato diplomová práce je zaměřena na návrh a realizaci semiaktivního RFID UHF tagu s hardwarovým generátorem náhodných čísel pro nízkopříkonové aplikace. Hardwarový generátor byl zkonstruován jako zařízení připojitelné k RFID UHF tagu, který dokáže díky této periferii přispět k vyšší bezpečnosti RFID technologie pomocí zvýšení entropie dat. Diplomová práce obsahuje potřebnou teorii pro realizaci zařízení a stručné zdůvodnění použitých komponentů. Zařízení generuje náhodná data a následně je posílá po SPI rozhraní do semiaktivního UHF RFID tagu. Pro generování náhodných čísel byla použita šumová dioda TESLA 36NQ52, která se dříve používala v můstkovém zapojení pro ladění antén. Celé zařízení je navrženo jako příslušenství pro semiaktivní UHF RFID tag. Komunikace se semiaktivním RFID tagem probíhá po sběrnici SPI (Serial Peripheral Interface), díky tomu se dá využít ke každému semiaktivnímu RFID tagu, který má toto rozhraní.

Klíčová slova:

RFID; generátor náhodných čísel; IoT; zabezpečení

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta elektrotechnická

Katedra telekomunikační techniky

Abstract:

This thesis is concentrated on the design and realization of Semi Active UHF RFID with random number generator for low-power applications. The harrdware generator is connectable device to RFID UHF tag which thanks to this periphery can lead to an increased security of the RFID technology. The thesis contains background theory which is necessary for the construction of the device and explains the justification of the components use in the implementation. The device generates random data which are send to the semi-active UHF RFID tag using SPI interface. In order to generate random numbers, TESLA 36NQ52 noise diode was used. This diode was previously used for bridging connections for antenna tuning. The entire device is designed as an accessory for the semi-active UHF RFID tag. The communication with the semi-active RFID tag is processed via the SPI.

Keywords:

RFID; random number generator; IoT; security

Obsah

1 Úvod

Technologie RFID (Radio Frequency Identification - Radiofrekvenční identifikace) slouží k rychlé bezdrátové radiofrekvenční identifikaci objektů na krátké vzdálenosti pomocí radiofrekvenčních vln. Tento způsob identifikace je jeden z nejstarších způsobů elektronické identifikace. Poprvé se tento způsob identifikace začal využívat již ve druhé světové válce, kdy byl využit v protivzdušné obraně. Radary upozorňovaly s předstihem pozemní jednotky na blížící se letadla. Pozemní jednotky však nedokázaly rozeznat, zda se jedná o vlastní vracející se letouny, či letouny nepřítele. Německá armáda jako první na světě učinila objev, že nakloněním letadla při návratu dojde ke změně odráženého signálu a díky tomu rozpoznají své letouny. Tuto metodu později rozšířily britské letové jednotky. Britové umístili na letouny vysílače (odpovídače). Tyto vysílače při přijetí radarového signálu z pozemní stanice vyslaly zpět k pozemní stanici signál s identifikací domácího letounu. Na tomto shodném principu pracuje i RFID. RFID čtečka nejprve vyšle signál směrem k RFID tagu a ten odrazí zpět signál do čtečky. Tento systém se nazývá pasivní RFID technologie. Existuje také RFID systém semiaktivní a aktivní. Semiaktivní systém pracuje právě na principu britské technologie označení letadel. RFID čtečka vyšle signál směrem k RFID tagu, ten ho přijme a následně vyšle na základě přijatého signálu odpověď. Aktivní RFID technologie vysílá informace do okolí neustále. Technologie RFID se se používá v nejrůznějších odvětvích a oblastech, jako je například zabezpečení budov, identifikace zboží na paletách, identifikace dobytka, elektronické průkazy, elektronická identifikace výrobků na výrobním pásu a podobně. Jeho největší výhodou je rychlost a přesnost zpracování informací. Za RFID zařízení můžeme považovat vše, co o sobě prozradí svoje ID, které lze přečíst po radiových vlnách. Pro bezdrátovou komunikaci je potřeba identifikátor – RFID tag a čtecí zařízení – RFID čtečka. Informace jsou uloženy v RFID tagu, z kterého vyčítá čtecí zařízení informace. Čtecí zařízení nečte informace po částech, nýbrž je čte všechny najednou. Tato vlastnost umožňuje načíst mnoho RFID tagů najednou. Například více zboží na paletě. Problémem těchto zařízení je komunikace mezi RFID čtečkou a vlastním tagem, která je většinou nezabezpečená. Pokud je již komunikace zabezpečená, tak za cenu velkého nárůstu pořizovací ceny RFID technologie.

Tato diplomová práce se zabývá tvorbou semiaktivního RFID UHF tagu s generátorem náhodných dat. Práce je dělena do dvou částí. První částí je teoretické zpracování informací potřebných pro realizaci zařízení. V těchto teoretických kapitolách popisuji princip funkce RFID technologie, problematiku generování náhodných dat nebo způsoby zabezpečení. Druhá část je zaměřená na praktickou konstrukci zařízení. V této části popisují dílčí kapitoly, výběr a uspořádání komponent, z kterých je konečný přípravek vytvořen. Poslední kapitolou týkající se praktické části je i popis a provedení.

Tato diplomová práce je součástí většího projektu zabývajícího se možností omezení neautorizovaného vyčítání dostupných dat nebo jejich pozměnění, a to v logistickém řetězci mezi dodavateli a odběrateli. Způsob zabezpečení se aplikuje až na přenosové trase mezi servery jednotlivých společností. Pro vytvoření tohoto zabezpečeného kanálu potřebujeme větší kapacitu dat, než produkuje samotné RFID v EPCglobal standardu. Největší výhoda tohoto návrhu zabezpečení komunikační trasy v logistickém řetězci je nevýrazné navýšení ceny. Pro aplikace standardních bezpečnostních protokolů je nutné mít dostatečnou kapacitu dat určených k zašifrování. Dostatečná data samo RFID neprodukuje. Struktura RFID dat je z pohledu zabezpečovacích protokolů relativně strohá. Je výhodné dodat další redundantní data pro využití šifrovacích algoritmů. EPCglobal standard produkuje data o velikosti 96 bitů a například nejběžněji používaný protokol TLS využívající symetrické šifry vyžaduje minimální velikost dat pro zašifrování 255 bitů. Z těchto důvodů je nutno k RFID tagu přidat zařízení, které doplní zbylý počet bitů generováním náhodných čísel. Díky této úpravě RFID tagu zvýšíme entropii dat dodávanou do šifrovacích algoritmů. Entropie se dá vysvětlit jako neuspořádanost nebo náhodnost dat. Entropie je pravděpodobnost možných stavů systému [1], [2].

2 RFID – Radiofrekvenční identifikace

2.1 Problematika zabezpečení RFID

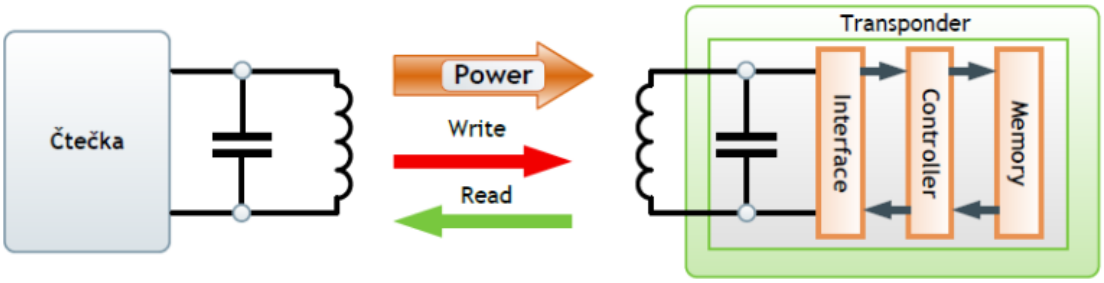
RFID slouží k identifikaci majetku, zařízení, osob a podobně. Při identifikaci osob jde o povolení vstupu do objektů, areálů, budov. Jedná se o zabezpečení vstupu do objektů. Technologie RFID většinou ale vlastní zabezpečení neobsahuje. Je to zapříčiněno hlavně vyšší pořizovací cenou při implementaci zabezpečení. V dnešní moderní době je potřeba si své soukromí chránit. Je-li RFID technologie umístěna ve výrobních halách, kde se nepředpokládá výskyt cizí osoby, která by mohla učinit neoprávněné vyčtení z bezprostřední blízkosti, tak vyšší úroveň zabezpečení řešit nemusíme. Zde jsou ID produktů chráněny plechovými stěnami hal a výrobních prostorů, které mají stínící účinek v řádu několika desítek dB. Dalším opatřením proti neoprávněnému vyčtení je i velký počet RFID tagů a tím zvýšená entropie a množství dat v éteru. Díky tomuto jevu nejsme schopni daný objekt zaměřit, natož určit, kde se v prostoru nachází. Proti útočníkovi zde máme výhodu rozlehlosti hal. V těchto rozlehlých halách není útočník schopný ani s nejcitlivějšími zařízeními vyčíst důvěrné informace. Tyto informace se ztratí v šumu. Šum je v halách vytvářen také vysokým počtem zařízení, velmi často pracujících na blízkých frekvencích. Vyjede-li však nákladní automobil se zbožím naloženým na návěsu, který je přikrytý pouze plachtou, tak se situace zásadně mění. Útočník se dokáže dostat do těsné blízkosti za automobil a díky tomu se ocitne v dostatečné čtecí vzdálenosti bez různých již dříve popsaných překážek. Útočníkovi nyní nic nebrání k bezproblémovému přečtení obsahu RFID tagů, a tak má dostupné informace, co daný automobil převáží a následně může tyto informace využít nežádoucím způsobem. Chceme-li, jako lidstvo v budoucnu využívat radiofrekvenční identifikaci pro identifikace objektů a zařízení v technologii Internetu věcí, nesmíme zapomínat na zabezpečení všech dílčích částí v komunikačním řetězci. Vždy byly a budou nejdražší a nejžádanější komoditou informace. Proto je musíme chránit!

Konstrukce RFID tagů neumožňuje příliš mnoho variant, jak daný typ komunikace zabezpečit. Je to zapříčiněno tím, že RFID technologie je cílená na co nejnižší spotřebu a nejvyšší životnost zařízení.

2.2 Dělení RFID dle typu tagu

2.2.1 Princip pasivního RFID tagu

Princip pasivních RFID tagů je takový, že čtečka je naladěna pomocí pasivních prvků na určitý kmitočtový rozsah. Tato frekvence, na kterou je rezonanční obvod naladěn, se nazývá nosná frekvence. Nosná frekvence je zkombinována pomocí modulace se vstupním signálem. Modulace je úprava vstupního signálu takovým způsobem, že se vstupní data, která nejsou v základním pásmu přenositelná, přizpůsobí předem definovaným způsobem tak, aby se mohla vysílat daným komunikačním kanálem s vhodnými parametry. Díky rezonančnímu obvodu je čtečka naladěná na určitou frekvenci a na této frekvenci je taktéž naladěn RFID tag pomocí rezonančního obvodu. Čtečka začíná vysílat energii (výkon) směrem k RFID tagu. V RFID tagu je cívka, která slouží jako anténa, která právě s dalšími pasivními prvky vytváří rezonanční obvod na dané frekvenci. Tento rezonanční obvod naváže přijatou energii do obvodu v RFID tagu a za pomoci kondenzátoru přijatou energii nějaký čas uschová. Z přijaté energie je napájen celý RFID tag. RFID tag pomocí dalších součástek upravuje přijatý signál a odesílá zpět odpověď do RFID čtečky.



Obrázek 1 - Komunikační řetězec RFID [3]

Z popsaného principu je vidět, že pasivní RFID tag nedisponuje velkým množstvím energie a proto se u pasivních tagů využívá součástek s co nejmenší spotřebou. Tyto obvody, aby měly co nejnižší spotřebu, musí být co možná nejprimitivnější. Nejprimitivnější obvodové struktury ale také nemívají příliš dostupné paměti, natož výpočetního či vysílacího výkonu. Pasivní tag má vlivem této jednoduché technologie, závislé na napájení z RFID čtečky, často malý čtecí dosah. Díky takto omezené kapacitě akumulované energie je pasivní tag z hlediska bezpečnosti spíše nevhodný. Zařízení rovněž nedisponují výpočetním výkonem ani dostupnou energií. Jeho nesporná výhoda však tkví v pořizovací ceně. Pořizovací náklady jsou oproti aktivní technologii zanedbatelné. Tento chip se hodí pro jednorázové identifikace předmětů, kdy se tagu po jeho službě ukončí život. Tento způsob je vhodný pro označení výrobků do obchodů. Slouží jako náhrada čárových kódů s využitelnějšími vlastnostmi. Technologii označování zboží pomocí pasivních RFID tagů využívá již dlouhá léta anglický obchod Marks & Spencer. Tento obchod byl průkopníkem ve značení zboží RFID tagem. Nově aplikovaná technologie RFID se stala velikou výhodu při inventuře, kdy se obsluha projde s RFID čtečkou pouze kolem regálů se zbožím a tím zjistí, jaké výrobky a počty kusů se nacházejí na prodejně či ve skladě. Zde je právě zmíněný problém se zabezpečením. Při používání čárových kódů musel člověk uchopit každý předmět a naskenovat čárový kód umístěný na zboží. Čárový kód také neobsahoval číslo daného výrobku, ale pouze identifikaci typu zboží. Při využití RFID tagů máme v tagu zaneseno i pořadové nebo výrobní číslo daného zboží.

2.2.2 Princip aktivního a semiaktivního RFID tagu

Třída aktivního RFID vznikla za účelem zvýšení čtecí vzdálenosti z několika centimetrů až metrů, která se vyskytovala u pasivní technologie RFID, na vzdálenost několika desítek až stovek metrů. U aktivních RFID tagů máme změnu principu napájení RFID tagu. RFID tag není napájen z vysílané energie od RFID čtečky, ale má svůj vlastní interní zdroj elektrické energie. Jako zdroj elektrické energie se používá baterie. Princip komunikace mezi zařízeními zůstává podobný, jako u pasivního tagu. RFID aktivní tagy se ale podle způsobu vysílání (odpovídání) dělí na další dvě podkategorie. První kategorie je semiaktivní RFID technologie a druhá je aktivní technologie. Semiaktivní tag pracuje na takovém principu, že RFID čtečka vyšle dotaz pro získání informací z RFID tagů. RFID tag je neustále napájen z baterie a vyčkává na dotaz čtečky. V okamžiku přijetí dotazu od čtečky RFID tag začne odpovídat nezávisle na energii ze čtečky. U aktivního tagu je princip takový, že vysílá svoje informace do okolí neustále. U obou principů získáváme úpravou napájení velkou výhodu ve zvýšení dosahu čtení. Bohužel s výhodami přicházejí i nevýhody. Hlavní nevýhodou je cena. Tag lze využít jen tam, kde jeho cena nepřevyšuje cenu zboží, nebo kde je možné opakované využití tagu. Typickým příkladem jsou aktivní RFID tagy ve výrobním procesu v automobilovém průmyslu, kde se na začátku výroby připevní na karoserii. V aktivním RFID tagu připevněném na karoserii je po celou dobu průchodu výrobní linkou uložena celá budoucí konfigurace automobilu. Postupným průchodem linkou se ke karoserii montují další zařízení a příslušenství. RFID tag zde slouží k synchronizaci linky, aby všechny díly byly připraveny ve správném pořadí k namontování. Mezi nevýhody patří i větší rozměr a snížená životnost vlivem baterie.

Velkou nevýhodou z jiného pohledu úhlu je zmíněná výhoda vyššího čtecího dosahu. U pasivní technologie se musela čtečka nacházet v blízkém okolí RFID tagu. Při aktivní technologii RFID začíná být problém s distribucí dat pouze ověřené osobě. U aktivního tagu je čtecí vzdálenost možná řádově několika desítek až stovek metrů. Při takovém poloměru čtecí vzdálenosti se objevuje riziko neoprávněného vyčtení. V popisu pasivního tagu bylo vysvětleno, že ke zhoršení vyčtení informací uložených v paměti tagu nám napomáhají různé překážky mezi RFID čtečkou a tagem. Překážkami jsou myšleny například plechové stěny,

interferenční rušení od jiné technologie a podobně. U aktivní technologie máme vysílací výkon mnohonásobně vyšší. U vyššího vysílacího výkonu nebudou překážky v prostoru tak výrazně zamezovat šíření signálu, jako u pasivní technologie. Přičemž plechové stěny hal jsou i v tomto případě dobrý pomocník při zamezení šíření signálu vně haly. Musíme počítat i s tím, že vždy není pravidlem umístění výrobků v hale. Výrobky či jiná zařízení se také velmi často nacházejí vně hal, a proto se komunikace musí zabezpečit proti neoprávněnému vyčtení informací uložených na RFID tazích jiným způsobem [2], [3], [4].

2.3 RFID dělení dle frekvenčního pásma

RFID se dělí dle kmitočtů, na kterých pracuje komunikace mezi čtečkou a tagem. Můžeme je dělit nejčastěji do tří základních skupin. Každá skupina se hodí pro jiné materiály. Některé materiály dané frekvence pohlcují, některé s nimi nijak neinteragují, některé materiály dokonce dané frekvence utlumují.

a) LF (Low frequency) – Nízké kmitočty v rozsahu 125 až 134 kHz, technologie vhodná pro přenosy na malou vzdálenost, která je asi do 20 cm.

   - Technologie vhodná pro označení například textilu, ropy, papíru, plodin, plastů, suchého i mokrého dřeva, předmětů umístěných ve vodě či různých tekutinách, identifikace různých kovů a grafitu, evidence dobytka (živých organismů)

b) HF (High frequency) – Vysoké kmitočty v pásmu 13,56 MHz, zde je větší čtecí vzdálenost, než u LF, a to do vzdálenosti maximálně 1m

   - Technologie se využívá hlavně pro docházkové systémy, přístupové systémy do budov, elektronické peněženky, elektronické kupony a podobně

c) UHF (Ultra High Frequency) – Velmi vysoké kmitočty v pásmu 860 – 960 MHz. U této podkategorie je čtecí vzdálenost ze tří základních skupin nejvyšší. Dosahujeme čtecí vzdálenosti v řádu jednotek metrů. Díky tak vysokému čtecímu dosahu oproti ostatním

dvěma skupinám je technologie nejlépe využitelná v průmyslu. Výše udané pásmo 860 – 960 MHz se dělí na další skupiny dle kontinentů:

a. Evropa 865,6 - 867,6 MHz

b. Čína – zde jsou dostupná dvě frekvenční pásma, a to 920,5 – 924,5 MHz a 840,5 – 844,5 MHz

c. USA a Kanada 902 – 928 MHz

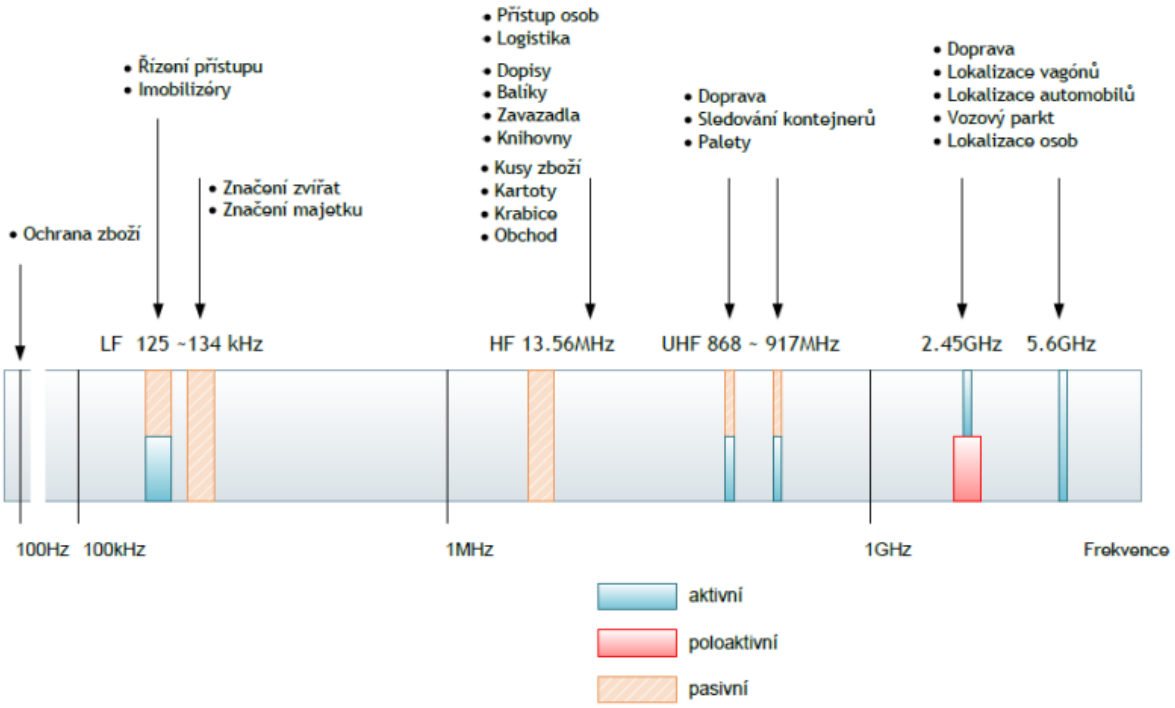
- Technologie se využívá pro identifikaci zboží na paletách, identifikace knih v knihovnách, identifikace výrobků na výrobním páse a podobně.

- S touto technologií je vyvinuto mnoho systémů, které dokáží sledovat zásilku již od výrobní linky přes logistiku k zákazníkovi. [5]

Existuje i čtvrtá skupina dělení RFID dle frekvenčního pásma, ale nepatří do základního dělení, a to z důvodů jejího malého využití v našich zeměpisných šířkách.

d) MW (Microwave) – Mikrovlnné pásmo 2,4GHz

- Využívání frekvence ve velmi zarušeném pásmu 2,4 GHz. Na nejbližším frekvenčním okolí dané technologie pracují dle podkladů od ČTÚ nejrůznější zařízení krátkého dosahu, jako je například Wi-fi v pásmu 2,4GHz, Bluetooth, RLAN (Radio Local Area Network) a jiné [6], [7], [8].



Obrázek 2 Frekvence používané různými aplikacemi RFID [3]

2.4 Struktura dat RFID tagu

V RFID standardech EPCglobal máme definovanou strukturu dat používanou v RFID tazích. Strukturu dat, kterou využívá RFID pro komunikaci nazýváme Electronic Product Code (EPC), kde jsou obsaženy tyto prvky:

a) **Záhlaví** – definuje délku, typ a strukturu kódu EPC
b) **EPC Manager** – identifikuje konkrétní společnost (výrobce)
c) **Object Manager** – identifikuje typ položky, druh výrobku a podobně
d) **Pořadové číslo** – identifikuje konkrétní položku v rámci daného druhu (typu) výrobku

GS1 EPCglobal je relativně nová skupina standardů, která kombinuje technologii RFID s komunikační infrastrukturou a kódem EPC. Standardy EPC vznikly z potřeby výměny dat mezi jednotlivými uživateli, popřípadě dodavateli a odběrateli zboží, kdy v minulosti nebyl formát dat uložených na RFID tazích nijak kontrolován, a tak docházelo k nejednoznačnostem

při načtení informací. Standardy byly vydány v roce 2003. Tyto standardy umožňují automatickou identifikaci a sledování položek v logistickém řetězci na lokální i globální úrovni, což vede k vyšší efektivitě a přehlednosti jednotlivých obchodních operací a procesů. [9]

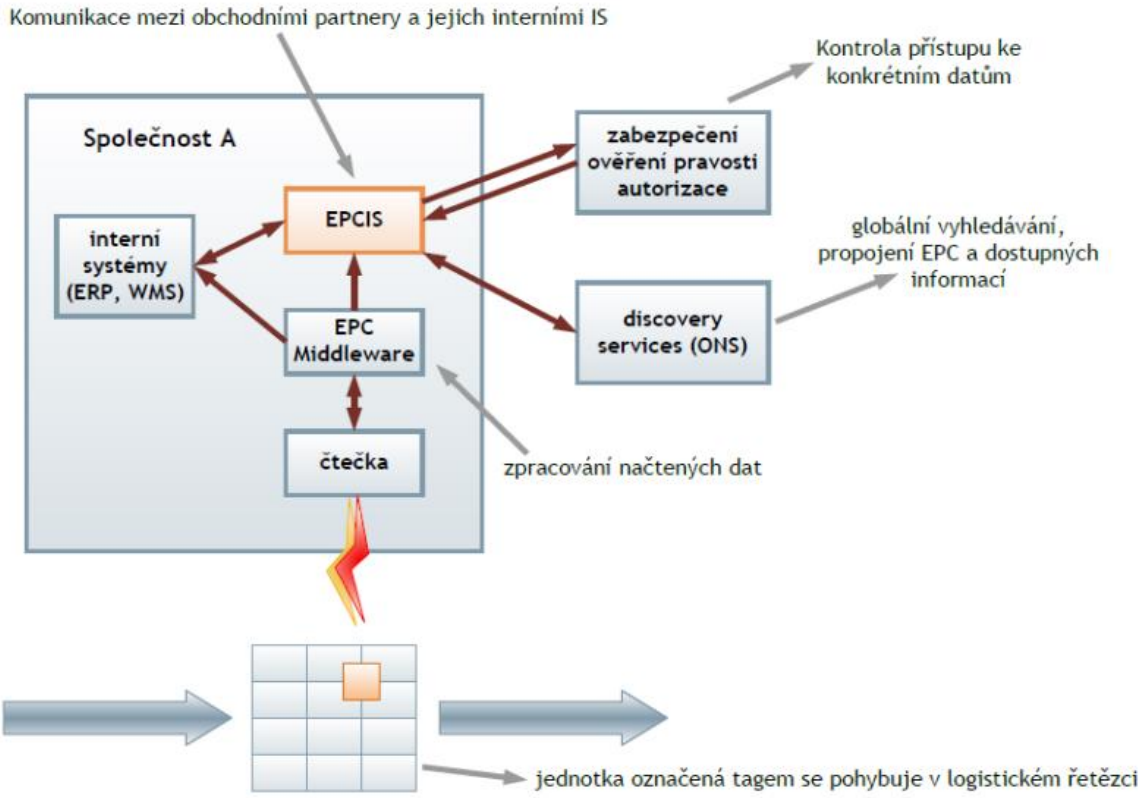
Organizace GS1 také klade důraz na ochranu osobních údajů, a to ještě před tím, než je nová cílová aplikace RFID uvedena na trh. Organizace se těmito kroky snaží o zvýšení důvěry a akceptovatelnosti koncovými zákazníky RFID technologie. [9]

Výměna dat mezi koncovými uživateli je zprostředkována pomocí komunikace mezi jejich servery, na kterých běží interní systémy. Komunikace musí probíhat v kanálu zabezpečeném proti odposlechu informace třetí stranou.

Princip komunikace:

1) Vyčtení EPC informace RFID čtečkou z RFID tagu
2) RFID čtečka předá EPC informaci do serveru EPC Middleware
3) Server EPC Middleware zpracuje data a poskytne je interním systémům a serveru EPCIS
4) Server EPCIS = Electronic Product Code Information Service – provádí procesy ověřování a hledání vlastností přečteného objektu s RFID tagem v centrální databázi ONS = Object Name Service
5) Server EPCIS následně provádí i ověření práv daného uživatele (RFID systému) pro přístup k datům

   [3]

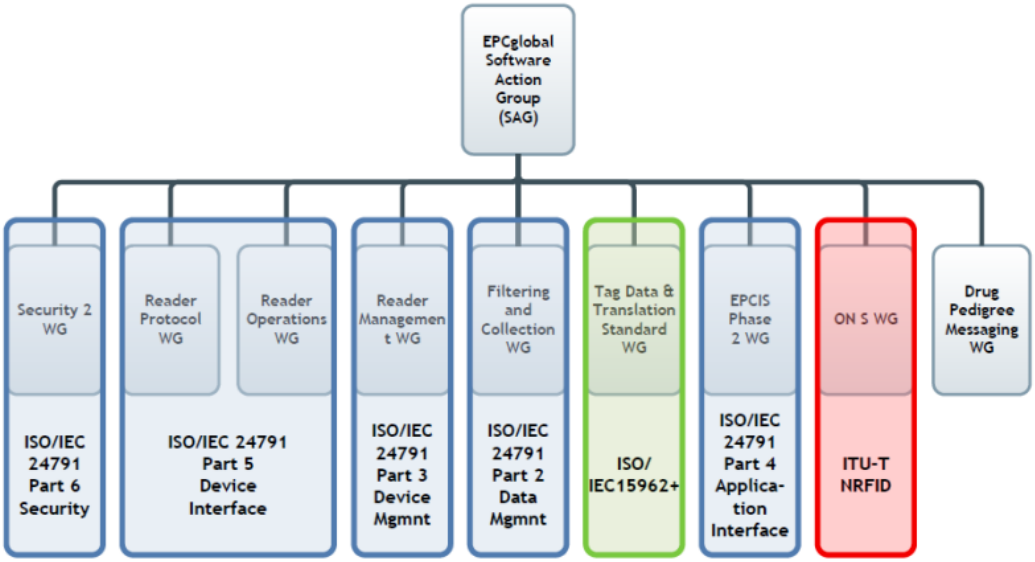


Obrázek 3 - Základní bloky komunikační sítě EPC global [3]

EPC global standardy se nezabývají pouze strukturou dat. Standardy popisují více částí systému. Ve standardech jsou předepsány tyto části [3]:

a) Bezpečnost
b) Hardware
c) Management systému
d) Management dat
e) Protokol přenosu dat
f) Aplikační rozhraní

Schématické znázornění dělení jednotlivých norem je popsáno na následujícím obrázku:



Obrázek 4 - Dělení jednotlivých standardů dle EPC global [3]

2.5 RFID a bezpečnost

RFID se v budoucnu bude čím dál více objevovat v nejrůznějších aplikacích, ať už to bude ve spojení s obchodním průmyslem, Internetem věcí nebo v úplně jiném odvětí. Nyní si nikdo z nás nedokáže představit, jak velký potenciál toto zařízení může mít díky neustále se zvyšujícímu čtecímu dosahu a spolehlivosti načtení RFID tagu.

Problém zde nastává v bezpečnosti. RFID není připraveno na zabezpečení. Dokonce někteří lidé tvrdí, že je toto zařízení nevhodné pro aplikaci zabezpečení. Toto tvrzení vyvstává z předpokladů, že RFID tagy jsou jednoduchá zařízení, která nedisponují přílišným výkonem a ani není tento výkon možné zajistit v nových zařízeních. Je to dáno tím, že zařízení musí mít, co nejnižší spotřebu. Princip napájení a spotřeby je popsán v dílčí kapitole 2.2.1 Princip pasivního RFID tagu a v kapitole 2.2.2 Princip aktivního a semiaktivního RFID tagu.

2.6 Princip aktivního a semiaktivního RFID tagu.

Bezpečnost RFID tagů se začala významně řešit až po upozornění od pana Lukase Grunwalda na konferenci Black Hat v roce 2004. Tento pán ukázal, jak snadno může hacker či jiný záškodník modifikovat data u přepisovatelných RFID tagů. Vyvinul program, pomocí kterého dokázal, že je schopen přečíst, pozměnit nebo dokonce přemazat celý RFID tag. Tento program nazval RFDump. Program RFDump pro svou činnost potřeboval pouze správnou RFID čtečku a PDA či notebook s operačními systémy Windows a Linux. Tento pán předvedl, jakou škodu by dokázal člověk napáchat, kdyby s tímto zařízením napochodoval do obchodu a začal by modifikovat data uložená v RFID tazích. Naštěstí se i v dnešní době, právě z bezpečnostních a cenových důvodů používají RFID tagy s podporou EPC standardů, na které se dá zapisovat pouze jednou. U těchto zařízení je pouze riziko vyčtení informace ze zařízení. U některých aplikací se ale nevyhneme použití zařízení s ISO standardy či se standardy EPC vyšších generací, kdy od druhé generace podporují tagy až několik tisíc přepsání.

Je zřejmé, že u přepisovatelných RFID tagů je začlenění bezpečnosti nezbytné. Může se zdát, že potřebujeme zabezpečit pouze přepis dat v RFID tagu. Ale bohužel, dnes může být problémem i pouhé vyčtení informace z tagu. Ve spojeni s Internetem věcí se RFID tagy mohou a budou masivně rozšiřovat. Musíme se tedy zamyslet nad dostatečným zabezpečením. Pokud budeme mít například v domácnosti označena nejrůznější zařízení RFID tagy, které budeme využívat pro různé aplikace a data by nebyla zabezpečená proti neoprávněnému vyčtení, natož přepisu, může nastat veliký problém. Vezmeme si jako příklad zloděje, který se dokáže dostat ke vchodovým dveřím do bytu, kde se bude nacházet již ve čtecí vzdálenosti zařízení s RFID tagem. V budoucnu se mohou RFID tagy nacházet například na veškeré elektronice a tak bude mít zloděj v případě nezabezpečené komunikace k dispozici seznam toho, co se v daném bytě nachází. Zloděj si například projde dům a naskenuje majetek umístěný ve všech bytech a následně se rozhodne, který byt bude pro něj nejvýhodnější vyloupit.

Samotnou kategorií v problému se zabezpečením byla zahraniční kauza obchodního řetězce Tesco. Prodejní taktika velkých obchodních řetězců je taková, že se zákazníkům snaží do jejich každodenní cesty při nakupování vložit ty výrobky, které potřebují aktuálně prodat.

Tento byznys plán je dnes velmi žádaný a vytváří se různé modely průchodů lidí za použití nejrůznějších technologií. Jednou takovou hojně využívanou technologií je technologie sledování a dopočítávání pohybu po obchodních domech nebo po prodejnách z mobilního signálu. Po obchodním centru nebo velké prodejně je rozmístěno více základnových stanic, díky kterým lze podle úrovně a směru šíření signálu dopočítat, kudy zákazníci nejčastěji chodí. Na stejném principu obchodní řetězec Tesco vytvořil podobnou technologii, kde umístili do uliček po celém obchodu mnoho RFID čteček a pokud zákazník projel pod čtečkou, zařízení zaznamenalo jeho průjezd kontrolním bodem a RFID čtečka tuto informaci poslala nadřízenému systému, který to zaznamenal do mapy obchodu. Výstupní informace z tohoto systému dávala informace provozovateli obchodu o největším výskytu a směru pohybu zákazníků. Využitím takto vypracovaných mapových podkladů je možné naplánovat, kam se zboží, které prodejce potřebuje urychleně prodat umístí. Z hlediska zákona o ochraně osobních informací je tento způsob zcela legální, protože se informace nespojují s danou osobou, ale pouze se tvoří anonymní modely s počty průchozích lidí. Proti tomuto typu získávání informací se nemůžeme chránit, protože dané zařízení je majetkem provozovatele a využívá ho k identifikaci zboží na pokladně. To, že ho využije i k tomuto lokalizačnímu účelu nejsme schopni zabránit. Proto i kdyby bylo zařízení šifrováno, tak provozovatel toto šifrování bude znát a může mít i tuto lokalizační službu šifrovanou.

Budeme-li se zabývat zabezpečením proti neoprávněnému zneužití cizí osobou, pak zjistíme, že na trhu již některá zabezpečení existují [1], [3], [4], [8].

2.6.1 Druhy zabezpečení:

Nejjednodušší možností zabezpečení UHF RFID technologie je, že po využití RFID tagu (například zaplacením zboží na kase) se RFID tag takzvaně usmrtí. To je provedeno metodou, která se nazývá soft blocker. Jedná se o metodu, která spočívá ve změně nastavení jednoho bitu na hodnotu jedna, nazývajícího se soukromý bit. Při nastavení tohoto bitu na úroveň 0 tag odpovídá na dotazy ze čtečky. Je-li bit nastaven na hodnotu 1, tak tag již nikdy čtečce neodpoví. Tento proces je nevratný. Další možnost, jak tag usmrtit je vyslat k RFID tagu vysokou úroveň

signálu. V RFID tagu je již dopředu obvod napočítán takovým způsobem, aby se při naindukování této vysoké úrovně obvod přepálil. Díky přepálení již obvod není funkční a neodpovídá na dotazy čtečky. Tento princip je taktéž nevratný. Způsob tohoto zabezpečení neochraňuje zařízení před neoprávněným vyčtením po dobu jeho aktivní činnosti.

Hlavní způsob zabezpečení RFID komunikace je v dnešní době princip vytvoření bezpečného komunikačního kanálu mezí čtečkou a tagem. Systém funguje na principu vytvoření bezpečného komunikačního kanálu na základě žádosti a následné odpovědi od tagu. Čtečka v první fázi vyšle žádost, na kterou jí RFID tag odpoví. Po provedení této operace se komunikace mezi zařízeními přepne do šifrované komunikace dle předem stanovených algoritmů. Pro šifrování komunikace se používají symetrické i asymetrické klíče. U asymetrické kryptografie se využívá Public Key Infrastruktura – PKI, která pracuje na principu ověření pomocí veřejného klíče. Toto zabezpečení dokáže snížit riziko neoprávněného vyčtení či přepisu dat v RFID tagu. Jednou z dalších možností je i šifrování celého RFID tagu respektive šifrování dat uložených v něm. Problémem každého šifrování je potřeba většího výpočetního výkonu v zařízeních na obou stranách. Pokud porovnáme technologii šifrování celého RFID tagu a šifrování pouze přenosu z hlediska výkonové kapacity, pak vychází lépe technologie šifrování přenosového kanálu. Je méně energeticky náročná a proto se tato technologie využívá častěji. Tato technologie je dostupná dle standardů pro EPC/RFID Tag Data Standard, Release 1.10 [10] od tagů EPC 2. generace. Nadále je dle těchto standardů implementovaná metoda zabezpečení, ne však přímo pro využití v průmyslových aplikacích, kdy RFID tag nemůže být přečten jakoukoli čtečkou, ale zařízení se musí před první komunikací mezi sebou spárovat. Tato technologie není příliš vhodná pro identifikaci v UHF pásmu, kde se tato zařízení nejčastěji využívají v průmyslových aplikacích. V průmyslových systémech se využívá radiofrekvenční identifikace na zboží nebo produkty, které se sledují či identifikují ve více různých čtečkách na několika místech. Tato místa jsou často od sebe velmi vzdálená a tak systém využívající párování čtečky a tagu není příliš vhodný. Systém není vhodný ani z pohledu množství a míst, kde jsou RFID tagy upevněny na zboží [4], [10].

Existují i jiné mechanismy zabezpečení RFID technologie. Většina metod se ale zabývá zabezpečením RFID komunikace v pásmu 13,56MHz. Právě v pásmu 13,56MHz se využívají aplikace, na které se musí klást několikanásobně vyšší třída zabezpečení. Těmito aplikacemi

jsou myšleny nejrůznější bezkontaktní platební transakce. Tento typ zabezpečení je určen normou ISO/IEC 14443-3:2016. V této normě jsou standardizovány víceúčelové RFID tagy navržené tak, aby podporovaly až 5 různých aplikací v jedné bezdrátové kartě nebo přívěsku. V praxi lze využít jednu kartu nebo klíčenku jako bezdrátový klíč pro vstup do domu, peněženku na běžná placení v obchodě, k nahrání digitálního kuponu na městskou hromadnou dopravu nebo permanentku do nějakého klubu či k identifikaci přístupu do zaměstnání. Aby všechny tyto aplikace bylo možné využívat, je implementováno hned několik bezpečnostních prvků. Bezpečnost je zajištěna proti vysledování transakcí, klonování obsahu tagu a proti neoprávněnému vyčtení dat. Využívá se zde například dynamického šifrování pomocí algoritmů 3DES a SHA-1 doplněných o algoritmus zabezpečení klíče ANSI X9.63. Díky těmto zabezpečením se pro každou transakci či operaci generuje unikátní 128 bitový klíč, díky kterému se komunikace v plně zašifrovaném kanálu zajistí proti odposlechu. Technologie také umožňuje zapnout funkci vzájemné autorizace zařízení.

Metod pro zabezpečení komunikace mezi RFID čtečkou a tagem je veliké množství. Většina z nich se specializuje na pásmo 13,56MHz. Pro UHF pásmo také existují některé metody zabezpečení, u kterých je ale problém s navýšením ceny každého RFID tagu vlivem potřeby vyššího výpočetního výkonu a větší spotřeby energie. Právě tato diplomová práce se zabývá ověřením nápadu, jak zvýšit úroveň zabezpečení a nezvýšit pořizovací náklady na RFID tagy.

Myšlenka je taková, že v prostoru, kde je vyšší koncentrace RFID technologie nebude muset být zabezpečení implementováno přímo do jednotlivých RFID tagů, ale bude jedno zařízení, které zvyšuje entropii dat v radiovém éteru. Díky zvýšené entropii nebude možné základní technikou určit, která data patří danému RFID tagu a nebude ho možné odposlechnout či přesně zaměřit v prostoru. Zařízení zajistí, že se v radiovém éteru zvedne míra neuspořádanosti dat a také se zvýší pozadí šumu. Hlavním důvodem, proč zvyšujeme entropii dat v éteru je, že algoritmy zabezpečující přenosy potřebují větší množství dat. RFID technologie jich moc nenabízí a proto jsou v našem experimentu do éteru dodaná náhodná redundantní data. Tato redundantní data napomůžou ke kvalitnějšímu zabezpečení RFID technologie bez výrazného zvýšení ceny semiaktivních RFID UHF tagů.

3 Náhodně generovaná data

Náhodně generovaná data používáme skoro všichni denně a ani si to mnohdy neuvědomujeme. Náhodná čísla jsou využívána například v kryptografii, v simulačních softwarech, hraní deskových her (hod kostkou) nebo v loterii.

Generování náhodných dat není tak jednoduché. Ve většině aplikací, hlavně tedy ve světě informatiky jsou náhodná data generována za pomocí funkcí k tomu připravených v jednotlivých programovacích jazycích. Problémem je zde ale fakt, že generovaná data jsou pouze pseudonáhodná. Tato pseudonáhodná data jsou generována pravidelným způsobem pomocí matematického vzorce, což znamená, že jsou generována předvídatelným způsobem. U názvosloví „náhodně generovaná data“ je problém s rozlišení významu. Nevíme, zda se při použití toho slovního spojení jedná o data pseudonáhodná či generovaná opravdu náhodně. V textu budu rozlišovat následující termíny týkající se generování náhodných dat: náhodně generovaná data – obecně náhodná, blíže nespecifikovaná vygenerovaná data; opravdu náhodně generovaná data – generovaná data pomocí opravdu náhodného generátoru čísel (true random number generator); pseudonáhodná data – generovaná pomocí pseudonáhodného generátoru čísel [11], [12].

3.1 Typy generátorů náhodných čísel

V předchozích větách jsme si nastínili problémy s náhodnými generátory. Musíme rozlišovat dva druhy náhodných generátorů. Prvním z nich je opravdu náhodný generátor čísel, pro který se používá zkratka z anglického jazyka TRNG (True Random Number Generator) a druhý, který se nazývá Pseudonáhodný generátor čísel, pro který se používá opět anglická zkratka PRNG (Pseudo Random Number Generator). Pseudonáhodné generátory jsou většinou tvořeny softwarovými programy. Tyto programy bývají realizovány počítáním různých algebraických výrazů nebo u těch jednodušších je tvořen výběrem z předem vytvořených tabulek. U této metody se vždy po nějakém čase výstupní data začnou opakovat. Naopak

generátory opravdu náhodných čísel jsou naprosto vždy hardwarovým řešením. Pro zpracování v infomačních technologiích je část náhodného generování tvořena hardwarovou části, která zpracovává fyzikální veličiny a následně je výstup z hardwarového zařízení zpracováván softwarovou částí [11], [12].

3.2 Porovnání generátorů náhodných čísel

Existují aplikace, pro které jsou vhodné pseudonáhodné generátory a naopak také existují aplikace, které jsou naprosto nevhodné pro použití pseudonáhodné posloupnosti. Pseudonáhodná posloupnost má sice vynikající účinnost v generování náhodných čísel, kdy náhodná čísla tento generátor generuje velmi rychle a ve velkém počtu. Nevýhodou je ale to, že jsou vygenerovaná čísla deterministická. Deterministický algoritmus je takový, který vždy vychází ze stejných výchozích podmínek. Další nevýhoda je, že po nějaké době se začnou data opakovat. V takovém případě říkáme, že algoritmus je periodický. Největší nevýhodou opravdu náhodného generátoru čísel je to, že generuje čísla pomaleji, než pseudonáhodný generátor. Má ale výrazné výhody, kde má naprosto opačné vlastnosti, než pseudonáhodný generátor. Opravdu náhodný generátor je nedeterministický a neperiodický.

Charakteristiky	**Pseudonáhodný generátor čísel**	**Opravdu náhodný generátor čísel**
Účinnost	Vynikající	Nízká
Determiničnost	Deterministický	Nedeterministický
Periodicita	Periodický	Neperiodický

Díky neperiodicitě a nedeteminističnosti opravdu náhodného generátoru se tento generátor výborně hodí pro aplikace, kde potřebujeme zajistit vysokou úroveň náhodných dat. Jde tedy o šifrování, tahání čísel v loterii a podobně. Naopak pseudonáhodný generátor se hodí pro aplikace, kde potřebujeme velmi rychle generovat náhodná čísla, která nemusí být vždy plně

náhodná a rozdílná. Využívá se na aplikace typu simulování a modelování nebo pro náhodný výběr skladeb v přehrávačích a podobně [11], [13].

3.3 Klasifikace náhodnosti dat

Náhodnost je pravděpodobnostní vlastnost a chceme-li zjistit, zda se jedná o data náhodná, či pseudonáhodná, existují testy, které nám tuto informaci pomohou zjistit. Testy dělíme do dvou skupin. První skupinu nazýváme testy klasickými, druhou skupinu testy teoretickými. Klasické testy jsou aplikovány přímo na posloupnost náhodných dat, testy teoretické se zabývají spíše návrhem a konstrukcí generátorů pro náhodná čísla. [12]

Testovaná data se pro test převedou do binární podoby. V technické praxi se testy vlastností programů pro generování náhodnosti dat provádějí velmi často a tak byly nejen z těchto důvodů vytvořeny standardy amerického úřadu pro standardy a technologie NIST. Druhou významnou testovací sadou je DIEHARD, která byla publikována Georgem Marsagliou také v USA, konkrétně na Floridě. Testy jsou balíčky dílčích statistických testů. Například u NIST je 15 balíčků statistických testů. U každé varianty testu jsou dílčí balíčky statistických testů řešeny individuálně a závisí na programátorech aplikací. Jednotlivé dílčí statistické testy zkoumají náhodnosti libovolně dlouhých posloupností, vytvořené buď hardwarovými nebo softwarovými generátory. Testy jsou zvolené tak, aby obsáhly nejrůznější odlišnosti a mohly tak prozkoumat danou posloupnost do nejmenších detailů [14], [13], [15].

3.3.1 NIST testovací sada

Testovací sada NIST obsahuje 15 dílčích statistických testů, které mají za úkol otestovat binární posloupnost vyprodukovanou náhodnými generátory. Testy jsou zaměřeny na statistické odchylky v testovaných posloupnostech. Tyto případné odchylky potvrzují nebo naopak vyvracejí náhodnost dat. Některé z testů obsahují i další podtesty.

Skupina balíčků statistických testů NIST:

1) Frekvenční test
   - Test rozdělení nul a jedniček při opravdu náhodné sekvenci dat je přibližně počet jedniček a nul přibližně shodný. Tento test je nejdůležitější, protože všechny následující testy se tímto testem řídí.

2) Test četnosti v bloku
   - Blok o velikosti M-bitů tento test rozdělí na jedničky a nuly. Pokud se četnost jedniček a nul rovná přibližně M/2, pak jsou testovaná data náhodná.

3) Test shodných sérií
   - Test na celkový počet nepřerušených úseků stejných bitů (1111…11 nebo 00……000) Na základě tohoto rozdělení počtu jedniček a nul test rozhodne, zda je frekvence změn jedniček a nul příliš vysoká nebo příliš nízká.

4) Test nejdelšího série v bloku
   - Délka nejdelšího řetězce jedniček 1..11 při rozdělení posloupnosti o velikosti bloků M. Test určuje, jestli je nejdelší série jedniček možná v náhodných datech či nikoli. Neočekávané hodnoty největší délky posloupnosti jedniček souvisí s nejdelší posloupností nul. Proto je tedy možné tento test vykonávat pouze na posloupnosti jedniček.

5) Test na hodnost binární matice
   - Test určuje hodnost submatic v rámci celé sekvence. Sekvence délky n je rozdělena na matici $M \times Q$, kde počet těchto matic bude roven $N = \frac{n}{M \times Q}$. Test hodnotí nezávislost mezi řadami konstantní délky v rámci vstupní sekvence.

6) Spektrální test
   - Test využívá diskrétní Fourierova transformaci, pomocí které zkoumá, zda jsou ve spektru obsaženy všechny složky. Pokud by nebyly, pak se nejedná o náhodně generovaná data.

7) Nepřekrývající se vzorové řetězce
   - Test na odhalení generátorů, které produkují mnoho stejných aperiodických frekvencí. Aperiodické frekvence se hledají podle vzorového okna řetězce, a pokud je tato posloupnost nalezena, okno se posune na následný bit po nalezeném vzorovém řetězci.

8) Překrývající se vzorové řetězce
   - Shodný test jako v bodě 7), jen se po nalezení posloupnosti posune okno pouze o jeden bit a ne o celý vzorový řetězec.

9) Murerův univerzální statistický test
   - Kontrola, zda se data mohou zkomprimovat bezeztrátově, aniž by došlo ke ztrátě informace a pokud ano, tak data nejsou náhodná.

10) Test lineární složitosti
   - Test má za úkol zjistit, zda je náhodná sekvence dat dostatečně složitá na to, abychom ji mohli označit za opravdu náhodnou.

11) Test sérií
   - Test sérií má za cíl zjistit, zda je počet výskytů 2^m m-bitových vzorců očekávatelný od náhodné sekvence. Vychází z předpokladů rovnoměrného rozložení vzorků a tudíž má každý m-bitový vzorek stejnou pravděpodobnost. Pro m=1 je tento vzorek shodný s frekvenčním testem č. 1)

12) Test přibližné entropie

- Stejný test, jako test sérií v bodě č. 11). Rodíl je pouze v tom, že test sleduje četnost vzorů sousedních délek m a m+1.

13) Test kumulativních součtů

- Test počítá střední vzdálenost od počátečního bodu (první vygenerované číslo) v průběhu náhodného generování. Tyto vzdálenosti test sčítá a porovnává s předem definovaným rozmezím hodnot, které vychází pro opravdu náhodná data.

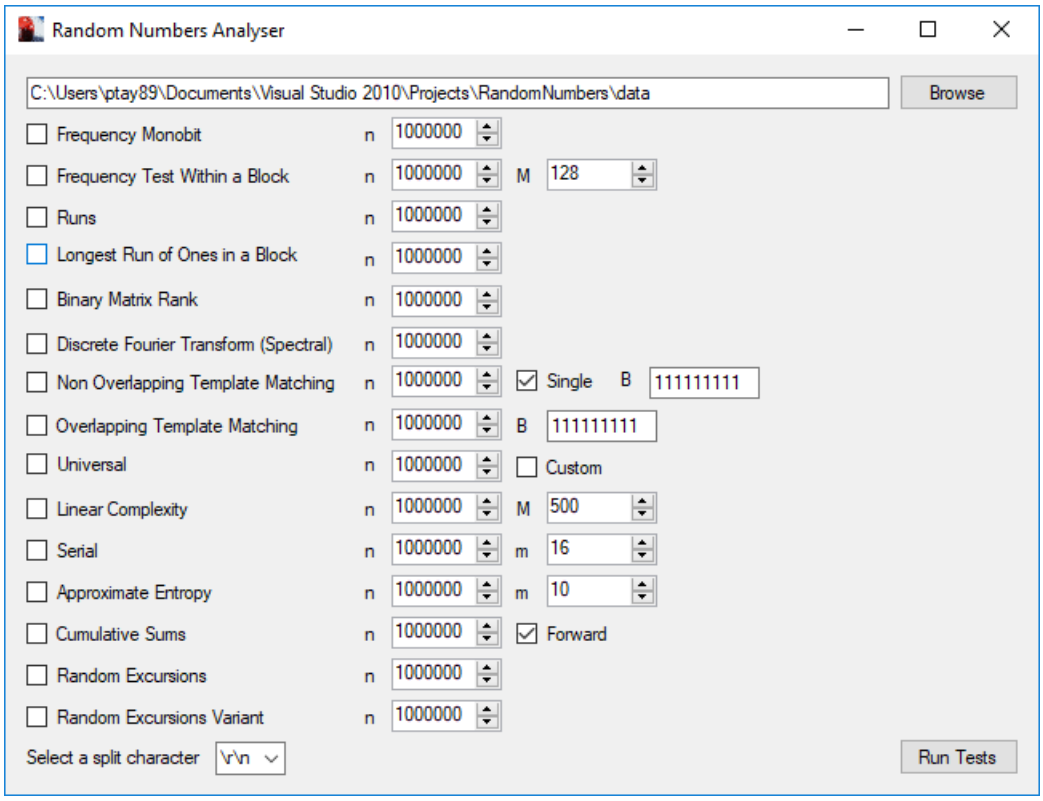
14) Test náhodné procházky

- Test počítá cykly, které se během testu komutativního součtu z bodu 13) navštíví přesně K-krát. Komutativní součet je odvozen od částečných součtů poté, co sekvence (0,1) je transformována na sekvence (1,1). Cílem tohoto testu je určit, zda počet návštěv jednotlivých stavů v rámci cyklu lze považovat za náhodný.

15) Variantní test náhodné procházky

- Cílem tohoto testu je určení odchylky od očekávaného počtu návštěv náhodné sekvence a rozhodnou, zda je vstupní posloupnost náhodná či nikoli.

Problémem u testu náhodnosti dat je závislost jednotlivých subtestů na těch předchozích. Je tedy potřeba tyto testy opakovat N-krát a hlavně na jiných náhodně vygenerovaných posloupnostech z daného zdroje. Tyto testy nejsou stoprocentní, protože jde vždy o statistický model testu. Pokud nebudeme mít dostatečný počet nezávislých vzorků, nemůžeme vyhodnotit závěr z proběhlého testování. Nastane-li situace, kde budeme mít pouze jeden vzorek dat a již neprojde první bod, který má za úkol rozdělení nul a jedniček, tak neproběhnou úspěšně ani následující subtesty, protože většina z nich je závislých na prvním bodě [14], [13] [15].



Obrázek 5 – Okno programu pro testování náhodnosti dat NIST

3.3.2 DIEHARD testovací sada

Testovací sadu DIEHARD vytvořil v posledním ročníku magisterského studia student Charmanaine Kenny na universitě Trinity College´s Management, kde studoval obor Science and Information systems Studies. Charmanaine Kenny se zabýval náhodnými čísly z různých online generátorů opravdu náhodných čísel. Tyto generátory jsou zárukou opravu náhodných čísel. Většina z nich generuje čísla na základě ověřených zdrojů pro opravdu náhodná čísla. Tyto generátory získávají náhodná data například měřením atmosférického šumu, měřením rozpadu radioaktivních částic a podobně. Charmanaine Kenny byl náhodností dat tak uchvácen, že si vzal starší studii od profesora Geore Marsaglia, který začal pracovat na projektu s názvem DIEHARD. Charmanaine Kenny začal pracovat na přepracování v rámci diplomové práce. Charmanaine Kenny tuto práci rozšířil a modernizoval. Nově tvořenou testovací sadu

DIEHARD neustále porovnával se standardy vytvořenými americkým úřadem pro standardy a technologie NIST. Výsledkem jeho diplomové práce byla testovací sada, o které tvrdil, že je lepší, než testovací sada NIST. Jeho závěrečná práce obsahovala dokonce i recenzi a kritiku testovací sady NIST. Charmanaine Kenny také vytvořil základ pro testování náhodnosti dat v reálném čase, který dnes využívají mnohé servery pro testování náhodných dat.

4 Šum

Pro zvýšení entropie dat v radiovém éteru budu potřebovat generovat opravdu náhodný šum. Pokud bych generoval pouze pseudonáhodný šum, pak by byl proces po dlouhé době sledování odhadnutelný.

Obecně je šum náhodné znečištění předem neurčeného signálu. Šum narušuje zpracování a přenos užitečného signálu. Je to velmi náhodný proces. Nachází se v různých oblastech a odvětvích. Například akustický šum, šum v digitálních fotografiích, šum v elektronice, komunikační šum a podobně. V elektronice se dokonce setkáváme s pojmem „Odstup signálu od šumu“.

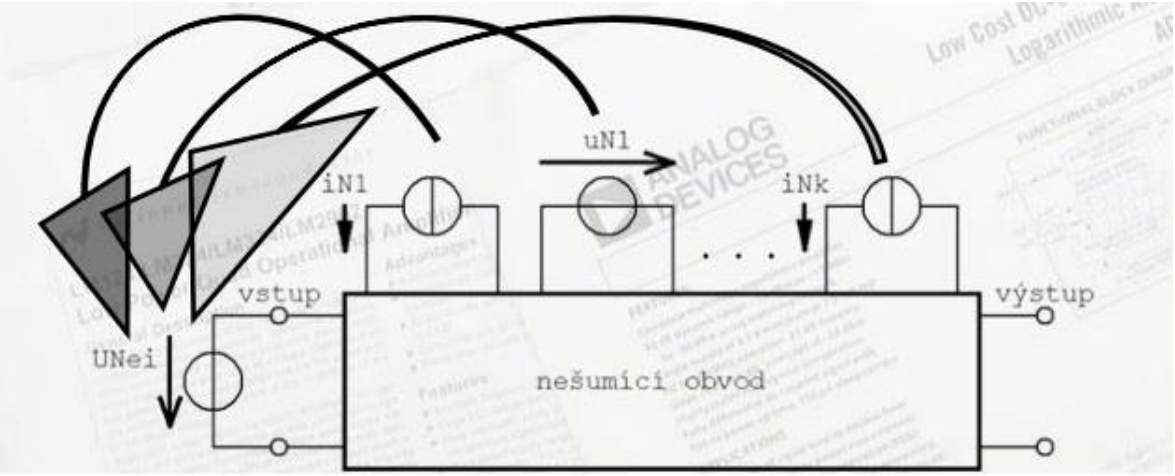
4.1 Šum v elektronice

V elektronice rozlišujeme dva druhy šumu [16] [17]:

a. Bílý šum – tento šum má rovnoměrné rozložení kmitočtových složek ve spektru

b. Barevný šum – tento šum má naopak nerovnoměrné rozložení kmitočtových složek ve spektru

Šum je velmi proměnlivý v čase a pro jeho klasifikaci se musíme podívat na jeho spektrum. Nejvíce nám o šumu vypoví jeho šumová spektrální hustota výkonu, protože spektrální charakteristiky šumu jsou v čase relativně stálé a tedy i dobře měřitelné. Chceme-li si šum vysvětlit a vymodelovat pomocí obvodových veličin, tak je lze modelovat pomocí rychle měnících se a neopakujících se hodnot na zdrojích napětí nebo zdrojích proudů. [16] [17]



Obrázek 6 - Šumový model obecného obvodu [16]

4.2 Analýza obvodu z hlediska šumu

Řešíme-li obecný obvod, budeme se snažit, aby daný obvod měl co nejnižší šum. V tomto obvodě chceme šum co nejvíce potlačit. Jelikož šum je velice náhodná veličina v čase, musíme obvod klasifikovat pomocí střední hodnoty výkonu, napětí a nebo proudu. Tato hodnota se nám při opakovaném měření nikdy nebude shodovat, a tak je tato hodnota spíše informativní a bude vypovídat pouze v případě, že se doba měření bude limitně blížit nule. Tato podmínka je ale v praxi neproveditelná, a tedy je toto hodnota spíše informativní [16].

$$U'^{2}_{N} = \frac{1}{T}\int_{t0}^{r0+T} U_N^2(t)dt \tag{4.1}$$

Rovnice popisuje střední kvadrát šumového napětí, kde U_N je šumové napětí, T je šířka měřeného pásma ve spektru a t0 je počáteční frekvence, od které začínáme zkoumat šum [16].

Na začátku odstavce jsem psal, že řešíme-li obecný obvod, budeme se snažit, aby měl daný obvod, co nejnižší šumové napětí U_N. Pro náš případ dané úlohy je ale potřeba, aby toto šumové napětí bylo co nejvyšší.

4.2.1 Tepelný šum

Tento typ šumu se vyskytuje ve vodičích i polovodičích a je všudypřítomný. Tento šum není závislý na napětí, proudu, ani na frekvenci. V našem rozdělení šumů v odstavci 4.1 klasifikujeme tento šum jako šum bílý. Tento šum vzniká při teplotě vyšší jak 0K náhodným pohybem elektronů ve struktuře krystalové mřížky.

Tepelný šum má rovnoměrné rozložení kmitočtových složek ve spektru a to až řádově do 100THz.

Šumové napětí se v našem zapojení nachází na rezistorech, propojovacích vodičích i polovodičových součástkách. Tepelný šum, ale pro vygenerování náhodných čísel moc nepomáhá. Tento šum je konstantní v celém spektru, které využíváme a Tepelný šum není závislý na změně vstupních veličin. Můžeme tedy tento druh šumu zanedbat. [17] [16].

4.2.2 Výstřelkový (Schottkyho) šum

Výstřelkový šum se vyskytuje u součástek s PN přechodem, kde je způsoben fluktuací nosičů náboje procházejícího potenciálovými bariérami v elektronických prvcích – uu PN přechodu průchod elektronů a děr přes PN přechod [17], [16].

$$i_n^2 = 2qI\Delta f, \tag{4.2}$$

kde q je elementární náboj $1{,}602\times10^{-19}$C, Δf je šířka pásma a I je „průměrný“ proud, který v důsledku tohoto typu šumu fluktuuje [17]

4.2.3 Blikavý šum

Tento typ šumu je způsoben hlavně ve struktuře krystalové mřížky. Konkrétně v poruchách jednotlivých vazeb v krystalové mřížce. Tento šum je chaotickým jevem = je velmi náhodný.

Šumová dioda 36NQ52 pracuje na tomto principu. Při výrobě byly záměrně narušeny vazby krystalové mřížky, které vyvolávají velmi náhodný šum.

Spektrální výkonová hustota proudu způsobeného pomocí blikavého šumu je dáno:

$$i_n^2 = k_f \frac{I^{\alpha_f}}{f} \Delta f, \tag{4.3}$$

de k_f a α_f jsou konstanty, jejichž hodnota se zajišťuje měřením a následnouidentifikací parametrů modelu [17]

Pro šumovou diodu 36NQ52 je $i_n = 6mA, k_f < 500\ (při\ 1{,}5V), \Delta f = 30MHz$

4.3 Využití bílého šumu v praxi

Bílý šum může být nejen nežádoucí, ale může nám i v některých případech pomoci. Díky bílému šumu můžeme testovat kmitočtové odezvy zesilovačů, elektrických filtrů a podobných obvodů. Můžeme také díky němu generovat náhodná čísla a to je přesně náš požadavek [16].

4.4 Zabezpečení přenosu RFID pomocí náhodného šumu

Na zabezpečení informace v radiovém prostředí se můžeme podívat také z pohledu šumu. To konkrétně tak, že budeme měnit odstup užitečného signálu v pozadí, které bude blíže nespecifikované a pro nás to tedy bude náhodný šum.

Pro vysvětlení znehodnocení vyčtení informace pomocí snížení odstupu signálu od šumu můžeme použít příklad, který určitě každý ze čtenářů zná. Při sledování televizního vysílání občas může dojít k takzvanému „zakostičkování“. Tento problém je ve většině případů způsoben snížením odstupu signálu od šumu. V běžné praxi se v radiovém prostředí nachází mnoho signálů, které jsou více, či méně posunuty ve spektru pro danou technologii v daném přenosovém pásmě. Tyto signály můžeme v našem případě připodobnit ke generátorům blíže nespecifikovaného náhodného šumu. Můžete však namítnout, že toto připodobnění problému neplatí, jelikož televizní kmitočty mají přesně dané kmitočty od ČTÚ a nemělo by tedy žádné rušení probíhat. V praxi to ale tak jednoznačné není. Sousední kanály se nepatrně překrývají s okolními kanály. Při tak vysokých výkonech jako je například vysílání LTE může k tomuto rušení dojít a běžně k němu dochází. Velikost „přelivu“ sousedního kanálu do sledovaného kanálu je závislá na poměrech jejich amplitud. Je-li úroveň sledovaného signálu daného kanálu několikanásobně vyšší, než je rušivý signál na sousedním kanále, tak z pohledu sledovaného signálu je sousední rušivý signál zanedbatelný a přelévá se do sledovaného signálu velmi nevýrazně. Nastane-li ale opačná situace, kdy bude nízká úroveň sledovaného signálu v určitém kanálu a rušivý signál v sousedním kanále bude několikanásobně vyšší, než sledovaný signál, může dojít dokonce k tomu, že celá šířka pásma sledovaného kanálu bude zakryta rušivým signálem. Obecně nejde určit, jak moc se rušivý signál přeleje do sledovaného kanálu. Toto rušení závisí na mnoha okolnostech, jako je šířka pásma daného kanálu, úroveň vysílaného signálu, způsob kódování signálu, provedení vstupních obvodů a podobně.

Vrátíme-li se k problematice zabezpečení RFID přenosu můžeme vyšší výkon nahradit vysíláním na kmitočtech určených pro RFID. Při koexistenci více funkčních RFID tagů v jednom místě dochází k překrývání jednotlivých kanálů a tedy k zahlcení spektra. Při tomto využívání a koexistenci více těchto zařízeních fungujících najednou jsme i tak schopni danou informaci přečíst, pokud známe identifikaci zařízení. Pokud ovšem identifikace (ID) zařízení neznáme, tak nastává problém s vyčtením této informace a následných dalších uložených dat v tomto zařízení. Myšlenka zabezpečení RFID pomocí přidáním jednoho či více semiaktivních RFID UHF tagů do prostoru vychází z této koncepce.

5 Internet věcí a RFID

Tato diplomová práce je součástí projektu, zabývajícího se problematikou zabezpečení Internetu věcí. V současnosti je Internet věcí, známý také jako IoT (Internet of Things) rychle se rozvíjejícím odvětvím v oblasti informačních a telekomunikačních technologiích. Do Internetu věcí se čím dál více začínají začleňovat veškeré stávající dostupné technologie. Jednou z těchto technologií je právě i RFID. V Internetu věcí se RFID technologie využívá nejvíce pro řešení dodavatelsko-odběratelských vztahů po celém světě. V této aplikaci se využívá komunikace mezi předměty a lidmi. Díky této definici spadá tato problematika také do Internetu věcí. Příkladem využití RFID technologie v Internetu věcí je pomoc, při logistickém řízení a časování například v automobilovém průmyslu, kde musí být daná komponenta připravená na výrobní lince k montáži někdy i s přesností jednotek sekund.

5.1 Co je vlastně Internet věcí?

Zařízení komunikují mezi sebou a nejen mezi sebou, ale i s nějakým řídícím systémem, případně i s člověkem. Internet věcí se nezabývá pouze propojením, mezi jednotlivými zařízeními, ale hlavně se jedná o nové typy služeb. Do Internetu věcí se mohou, a také se velmi často promítnout stávající služby, které již u některých zařízení využíváme. Mnohdy ale není například u těchto služeb taková dostupnost po celém našem území, jakou bychom potřebovali. Některé služby se mohou přesunutím ze stávajících sítí do sítě Internetu věcí zlevnit. Zlevní se díky tomu, že dosavadní technologie například komunikuje velmi nehospodárně na běžné síti, ať už se jedná o internet nebo o mobilní síť. Zařízení komunikující právě prostřednictvím sítě Internetu věcí mají relativně nízkou přenosovou rychlost v řádu stovek bitů za sekundu. Tato přenosová rychlost je pro tento účel dostačující. Většinou zařízení dostávají pouze povely, či informace. Zařízení sama o sobě komunikují jen velmi zřídka. Služby v Internetu věcí nejsou nijak striktně dány, či omezeny.

5.2 Bezpečnost v Internetu věcí

V zajištění bezpečnosti, ať už jde o jakoukoli technologii, jde vždy o kompromis mezi náklady na zabezpečení a škodou, která může vzniknout po narušení bezpečnosti. Ve světě Internetu věcí se na bezpečnost pamatuje při tvorbě systémů. Jsou zde ale stále dostupná nová zařízení, která jsou určená primárně pro aplikace, kde se zabezpečovat buď nevyplatí, nebo na zabezpečení zařízení ve fázi vývoje nikdo nepamatoval, či by systémem zabezpečení zařízení ztratila své výhody a přednosti. U těchto zařízení při použití v Internetu věcí je potřeba toto zabezpečení alespoň na základní úrovni doplnit. V Internetu věcí se musíme řídit poučkou, že čím je větší počet uživatelů dané aplikace, tím je tato aplikace zranitelnější. Důvodem je právě vyšší počet uživatelů, který je ohrožen statisticky větším počtem útoků, ale také větším zájmem od samotných útočníků, kteří mohou z dané služby cosi vytěžit. U Internetu věcí nesmíme pohlížet na dílčí součástky, ale musíme se na bezpečnost Internetu věcí dívat, jako na komplexní systém. Nesmí být podceněno zabezpečení žádné dílčí součástky či zařízení [3], [18].

6 Kryptografie

Kryptografie se zabývá návrhem a konstrukcí kryptografických algoritmů a způsoby jejich využívání. Kryptografie je podskupinou Kryptologie. Kryptologie je vědní obor, zahrnující kryptografii a kryptoanalýzu. Kryptoanalýza se zabývá metodami získávání otevřeného textu (nezabezpečených dat) z textu šifrovaného (zabezpečených dat). Kryptoanalýza zkoumá odolnost a zranitelnost kryptosystémů [19], [20].

V dnešním moderním světě je mnoho informací vytvářeno, udržováno a přenášeno v elektronické podobě. Mohou se tak velmi jednoduše stát cílem útočníků. Elektronické informace se dnes využívají k různým činnostem. Některé činnosti jsou více problematické z hlediska ochrany dat, některé méně. Mezi nejcitlivější informace, které musíme chránit kryptografií se řadí dnes už běžně využívaný elektronický styk s úřady, kde se dokonce často přenáší i náš elektronický podpis. Velice citlivá komunikace probíhá u bezkontaktní platby pomocí platební karty či jiného RFID zařízení. Nejsou to ale pouze tyto aplikace, které potřebujeme šifrovat. V dnešním rychle se rozvíjejícím světě je potřeba zabezpečit vše, co by se dalo nějak zneužít. Neméně toto platí i v odvětví Internetu věcí. V Internetu věcí se plánuje využívání globální infrastruktury a sdílení informace na jedné síti. V Internetu věcí jsou mnohé informace velmi cenné a citlivé, proto se musí i zde šifrovat.

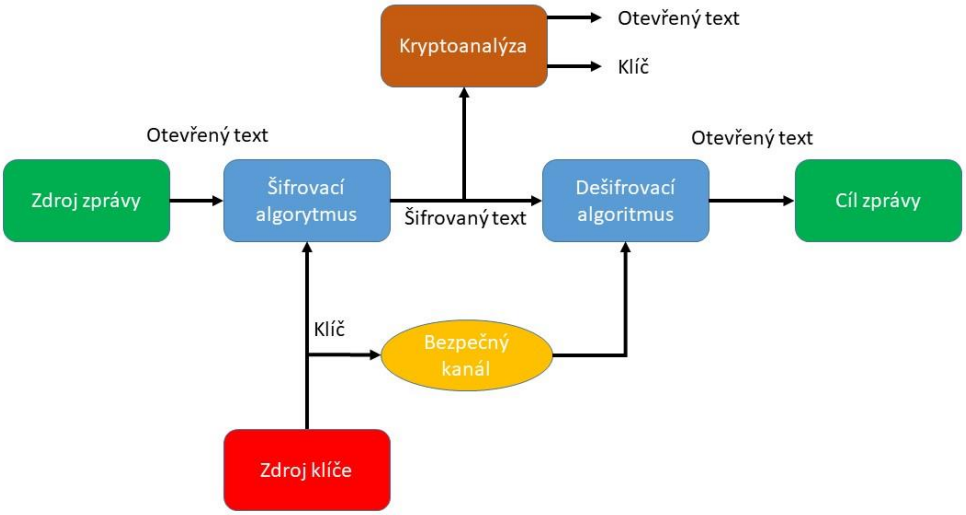
6.1 Princip šifrování

Na straně, kde potřebujeme zašifrovat data, máme zdroj zprávy. Zdroj zprávy jsou nezašifrovaná data, která nazýváme otevřený text. Otevřený text přivedeme na vstup šifrovacího algoritmu, který vytvoří z otevřeného textu šifrovaný text pomocí klíče. Klíč je generován zdrojem klíče.

Na přenosové cestě přenášíme zašifrovaný text. Na stranu, kde provádíme dešifrování, musíme přenést i informaci o použitém klíči. Tento klíč se distribuuje zabezpečeným kanálem. Zabezpečeným kanálem se myslí například sdělení si klíče mezi koncovými uživateli mimo

hlavní komunikační cestu. Na přenosové cestě může útočník použít kryptoanalýzu, pomocí níž dokáže útočník zjistit otevřený text bez znalosti klíče. Zde existují různé typy útoků.

Na straně dešifrování přijmeme šifrovaný text. Tento text přivedeme na vstup dešifrovacího algoritmu. Tento algoritmus převede šifrovaný text zpět na otevřený text za pomocí klíče, který byl k dešifrovací straně distribuován bezpečným kanálem.



Obrázek 7 - Shannonův model kryptosystému

6.2 Typy šifrování

Existuje několik bloků, do kterých můžeme šifrování rozdělit.

1) Klasické šifry:

a) Substituce – nahrazení textu za tajný text, který nedává smysl, jedna z nejprimitivnějších metod šifrování je realizována například prostým posuvem

b) Transpozice – zpřeházení písmen v prostoru, například navinutí papíru na tyč, kde je klíčem pro dešifrování zprávy poloměr tyče

Obrázek 8 - Transpoziční šifra Scytale - využívaná 500let př.n.l. [21]

c) Kombinace substituce a transpozice

2) Moderní šifry:

a) Symetrická šifra – šifrovací algoritmus, který využívá pro šifrování a dešifrování jeden a tentýž klíč

b) Asymetrická šifra – šifrovací algoritmus, který využívá pro šifrování a dešifrování dva různé klíče

3) Hašovací funkce

6.2.1 Symetrické šifry

Symetrické šifry se dále dělí na proudové a blokové. Proudové šifry zpracovávají data po bitech. Veliká výhoda proudových šifer je v hardwarové implementaci, která nám zajistí velkou rychlost zpracování. Proudovou šifru A5 využívají ke své činnosti například mobilní telefony. Další symetrickou šifrou je proudová šifra RC4, která se využívá pro zabezpečení Wi-Fi, SSL/TLS, Ipsec. Blokové symetrické šifry se zpracovávají po blocích konstantní velikosti 128b, kde je již nutná softwarová implementace. Blokové šifry jsou tedy v porovnání s proudovými pomalejší. Příklady blokových symetrických šifer jsou DES, 3DES, AES [19].

6.2.2 Asymetrické šifry

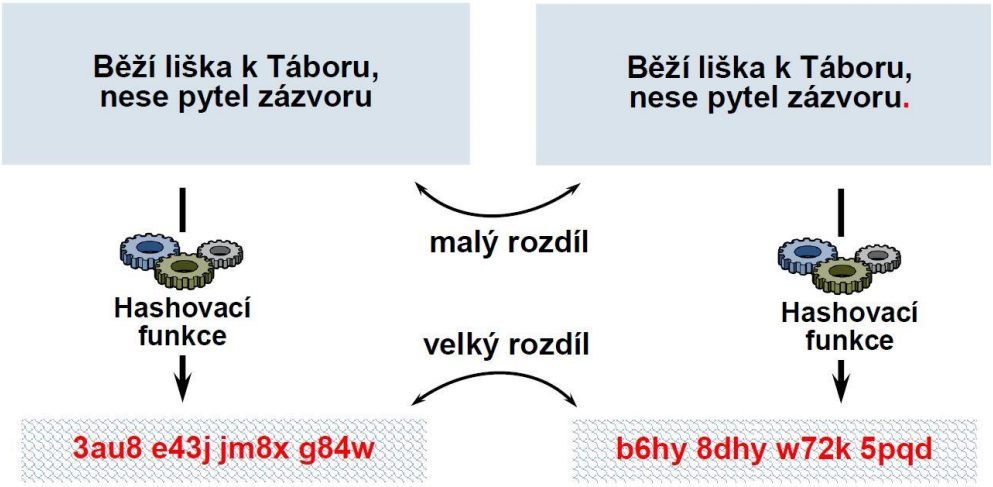
Asymetrická šifra znamená, že šifrovací algoritmus využívá pro šifrování a dešifrování dva různé klíče:

d) Veřejný klíč – jeden ze dvou klíčů používaných u asymetrické šifry, většinou využívaný pro šifrování, tento klíč nemusí být utajován
e) Soukromý klíč – druhý ze dvou klíčů používaných u asymetrické šifry, většinou využívaný pro dešifrování, klíč musí být vždy utajován

Asymetrické šifry lze využít nejen pro šifrování a dešifrování, ale také pro podepisování elektronických dokumentů (digitální podpis) a pro výměnu klíčů pro symetrické šifry. Asymetrická šifra je řádově 100-1000x pomalejší, než symetrická šifra. Asymetrická šifra má dlouhé klíče 1024 – 4096 bitů [19].

6.2.3 Hašovací funkce

Hašovací funkce je matematická funkce mapující libovolně dlouhý vstup, který musí mít konečnou délku, na výstup konstantní délky. Velikou výhodou této funkce je, že malá změna na vstupu vede k velké změně na výstupu. Typické velikosti výstupů jsou 160-512 bitů. Hašovací funkce má relativně rychlý výpočet. Používá se velmi často k zajištění integrity zprávy [19].



Obrázek 9 - Princip hašovací funkce [19]

6.3 Bezpečnost šifrování

Šifrování je velmi náročné na výpočetní výkon, na spotřebu energie a tudíž se s dobrým šifrováním velmi výrazně zvedá i cena koncového zařízení využívajícího různé mechanismy zabezpečení. Při využití šifrování chceme dosáhnout takového zabezpečení, aby nikdo na světě nebyl schopen toto zabezpečení prolomit. Toto zabezpečení se nazývá nepodmíněná bezpečnost a není příliš reálné. Existují dva pohledy na bezpečnost:

- Nepodmíněná bezpečnost – bezpečnostní šifru nelze prolomit bez ohledu na dostupné zařízení jakéhokoli výpočetního výkonu, a to z důvodu, že nám

šifrovaný text neposkytuje potřebné množství informací potřebných k jednoznačnému rozpoznání otevřeného textu.

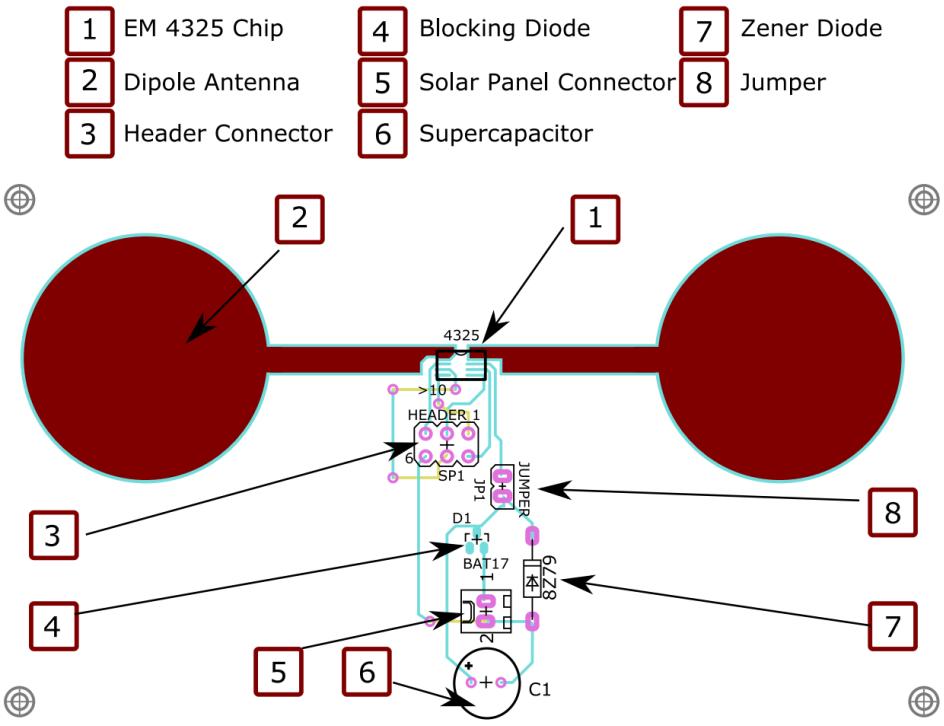
- Podmíněná bezpečnost – neprolomitelnost šifry spočívá v důvěře, že nemáme k dispozici dostatečné prostředky pro její prolomení. Dostatečnými prostředky se myslí, že nemáme dostupný výpočetní výkon nebo čas k jejímu prolomení. Tato teorie vychází z předpokladů, že cena na prolomení šifry je mnohonásobně vyšší, než cena získané informace. Kdyby byl tedy použit přístroj srovnatelné ceny, který by měl kvůli pořizovací ceně nižší výkon, tak čas nutný k prolomení šifry významně přesahuje dobu životnosti chráněné informace.

Základem šifrování je všeobecně známá poučka, která nám říká: „utajení šifrovacího algoritmu nesmí sloužit jako opatření nahrazující nebo garantující kvalitu šifrovacího systému."

Vysvětlení této poučky je takové, že útočník zná celý kryptosystém. Do detailů jsou mu známé kryptografické algoritmy a pouze klíč je tajný. V praxi se často vyskytovaly šifrovací metody, které měly utajované i algoritmy. Jak už tomu tak bývá, tak nikdy utajované algoritmy nezůstanou tajné navždy. U utajovaných algoritmů se velmi často po odhalení ukázaly bezpečnostní chyby. V okamžiku, kdy je algoritmus veřejný, dokáží vývojáři, kteří tyto algoritmy studují či přímo využívají, tyto bezpečnostní chyby včas odhalit a opravit [19], [20].

7 Návrh zařízení

Návrh a konstrukci zařízení jsem si rozdělil na dvě větší části. V první části jsem se věnoval tvorbě náhodného generátoru dat. Jedním z požadavků pro správný chod zabezpečení systému bylo, aby náhodně generovaná data byla opravdu náhodná a nejen pseudonáhodná. Poté, co jsem zjistil všechny potřebné informace k tvorbě opravdu náhodného generátoru, jsem přistoupil k druhé části, ve které jsem se zabýval digitalizací dat a následném zpracování dat pro odesílání do semiaktivního RFID UHF tagu. Semiaktivní RFID tag nebyl v této práci navrhován, protože byl využit již vyvinutý semiaktivní RFID UHF tag na katedře telekomunikací, fakulty elektrotechnické, ČVUT v Praze. Tento tag byl na fakultě navržen v práci, která se zabývala návrhem solárního semiaktivního RFID tagu [22].



Obrázek 10 – Layout semiaktivnído RFID UHF tagu navrženého na katedře telekomunikací, fakulty elektrotechnické, ČVUT v Praze [22]

Při zamyšlení se nad prvním bodem generování náhodných dat jsem si uvědomil, že musím začít zamyšlením nad druhou částí. Bylo nezbytné prozkoumat způsoby komunikace mezi mikroprocesorem a semiaktivním RFID UHF tagem. Po prozkoumání dokumentace jsem zjistil, že RFID tag od EM Microelectronic typ EM4324 bude vhodnější, protože disponuje komunikačním rozhraním SPI. V návrhu zařízení z předchozí práce na katedře telekomunikací již byl vytvořena deska s vyvedením SPI rozhraním z čipu EM4324. Díky vyvedenému SPI mohu navázat na tuto práci a použít mikroprocesor, který bude splňovat tyto požadavky:

Procesor musí disponovat právě SPI rozhraním pro připojení k RFID tagu, A/D převodníkem s dostatečnou rozlišovací schopností pro digitalizaci náhodného šumu a bude mít i malou spotřebou.

7.1 Požadavky a výběr mikroprocesoru

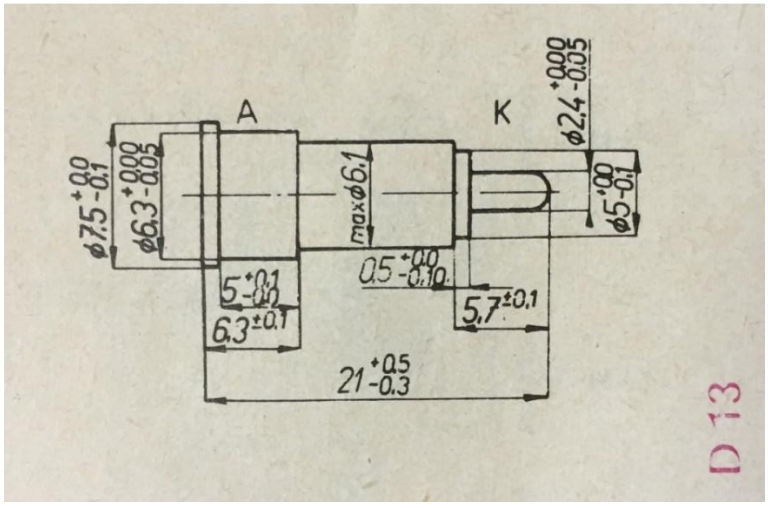
Při výběru mikroprocesoru jsem největší důraz kladl na velmi malou spotřebu. Malá spotřeba je nutná, protože tato aplikace musí být provozuschopná pouze na baterii. Dále je potřeba, aby mikroprocesor uměl komunikovat pomocí SPI protokolu, pomocí kterého bude komunikovat se semiaktivním RFID UHF tagem. Do užšího výběru byly zahrnuty dva mikroprocesory. Jeden od firmy Microchip a druhý od firmy STM. Obě firmy nabízejí malopříkonové mikroprocesory (Low power). Obě firmy měly na výběr z více druhů těchto procesorů, a nakonec při porovnání vycházely procesory od obou firem podobně. Měly srovnatelnou spotřebu i výpočetní výkon a paměť. Zvolil jsem mikroprocesor od firmy STM, a to konkrétně STM8L152C6. Tento mikroprocesor prodává firma již osazený na vývojové desce STM8L-DISCOVERY, která je pro můj úkol velmi vhodná. Díky této desce tedy odpadá složitý návrh plošného spoje a jeho následné osazení mikroprocesorem, které by připadalo v úvahu u procesoru od firmy Microchip. Tato vývojová deska obsahuje i velmi užitečnou funkci pro odladění při vývoji a tou je měření spotřeby procesoru. Tento procesor spotřebovává v režimu spánku cca. 0,35µA a v dynamickém režimu používání cca. 180µA/MHz. Pro porovnání spotřeby v režimu spánku a v režimu používání procesoru je nutné vysvětlit fakt, že spotřeba procesoru je velmi závislá na vytížení procesoru. Čím více operací daný procesor bude

vykonávat, tím se zvedne i jeho pracovní frekvence a bude se zvětšovat úměrně i spotřeba. Je tedy nutné na tento fakt brát ohled i při návrhu programu.

Obrázek 11 - Vývojová deska STM8L-Dicovery [23]

7.2 Generování náhodných dat pro procesor

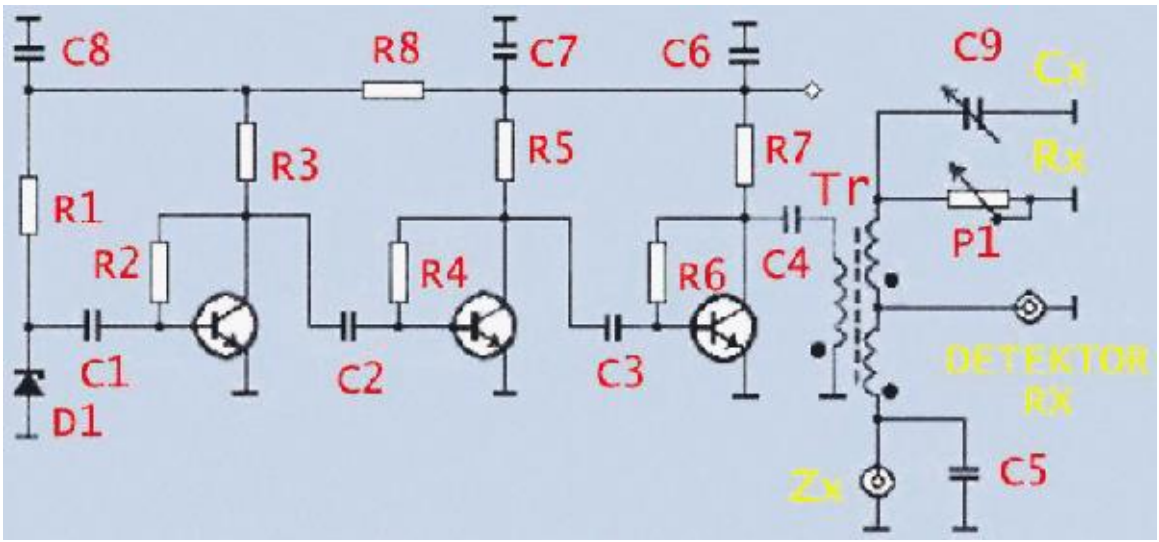
Nyní se vrátím k první části generování náhodných dat. První myšlenka, jak generovat náhodná data byla taková, že se budou generovat opravdu náhodná data v reálném čase. Bylo zapotřebí vymyslet, jakým způsobem se náhodná data budou generovat. Nápadů bylo hned několik. Jedna z prvních myšlenek byla generovat šum pomocí nezatíženého vstupu na A/D převodníku. Po přečtení odborných článků jsem usoudil, že by tento šum nebyl dostatečně náhodný. Byl by pouze pseudonáhodný, respektive by se za určitých podmínek mohl opakovat a tak byla tato myšlenka zavrhnuta. Nápad, který přišel následně, byl způsob zapojení tranzistoru KC507 v inverzním režimu. Tranzistor KC507 se vyráběl v souměrných vrstvách polovodičů. Inverzní režim znamená, že se zamění kolektor a emitor. Báze je polarizovaná v propustném směru. Díky tomuto zapojení vzniká druhotný produkt, kterým je šum. Tento nápad byl bohužel taky vyloučen. Pustil jsem se do hledání odborných článků o generování náhodného šumu v Amatérském rádiu ve vydání od roku 1976-1995. V části s diskrétními součástkami a praktická zapojení pro nf zesilovač jsem našel schéma zapojení se šumovou diodou 36NQ52, která se v minulosti používala do šumových můstků pro měření a seřizování antén. V dnešní době se již tato šumová dioda nevyrábí a ani se již pomocí tohoto zapojení antény neseřizují. Po pečlivém hledání a shánění jsem dva kusy zakoupil ze starších soukromých zásob.



Obrázek 12 - Typ pouzdra šumové diody 36NQ52 [24]

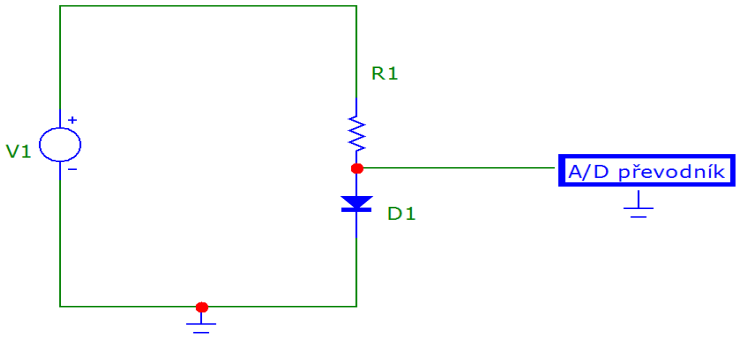
7.3 Zapojení pro generování náhodných dat

V tuto chvíli jsem měl vybranou a prostudovanou problematiku generování náhodných dat pomocí šumové diody. Přišel tedy čas na otázku, jak modifikovat původní zapojení šumového můstku.



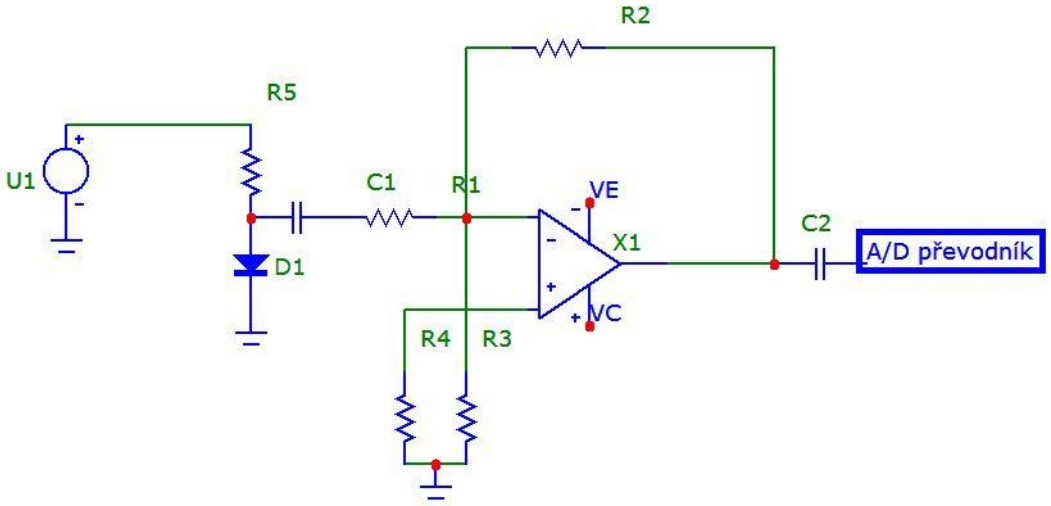
Obrázek 13 - Schéma zapojení šumového můstku [25]

Zapojení potřebuji upravit takovým způsobem, aby bylo možná co nejjednodušší, aby mělo co nejméně pasivních prvků, které by spotřebovávaly zbytečně elektrickou energii. Provedl jsem tedy několik pokusů se zapojeními. Začal jsem tím nejjednodušším možným.



Obrázek 14 - Schéma zapojení šumové diody - varianta 1

Po změření úrovní šumu bylo jasné, že takovéto jednoduché zapojení není možné. Vytvořil jsem následně nové zapojení s invertujícím operačním zesilovačem.



Obrázek 15 - Schéma zapojení šumové diody s invertujícím OZ-varianta 2

Po zapojení šumové diody s invertujícím OZ bohužel nastaly problémy s nízkou úrovní generovaného šumu. Nízká úroveň šumu byla zapříčiněna tím, že generovaný šum se nachází ve vyšším frekvenčním pásmu. V pásmu, které dokážu změřit na vstupu A/D převodníku mikroprocesoru je amplituda měřeného šumu velmi nízká. Šumová dioda z hlediska své konstrukce produkuje šum hlavně na vyšších kmitočtech. Tento problém jsem vyřešil použitím přístrojového operačního zesilovače, který má veliké zesílení a používá se také například pro zesilování biologických signálů. Díky tak obrovskému zesílení vnese zesilovač další zkreslení šumem, tím pádem se i zvýší náhodnost dat na výstupu. V mém případě jsem použil přístrojový zesilovač od firmy Analog Devices AD620.

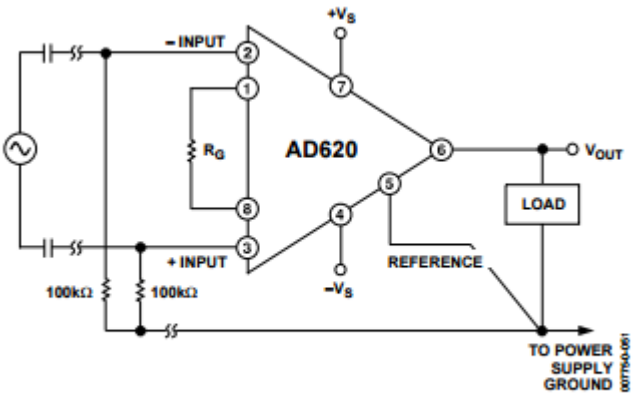
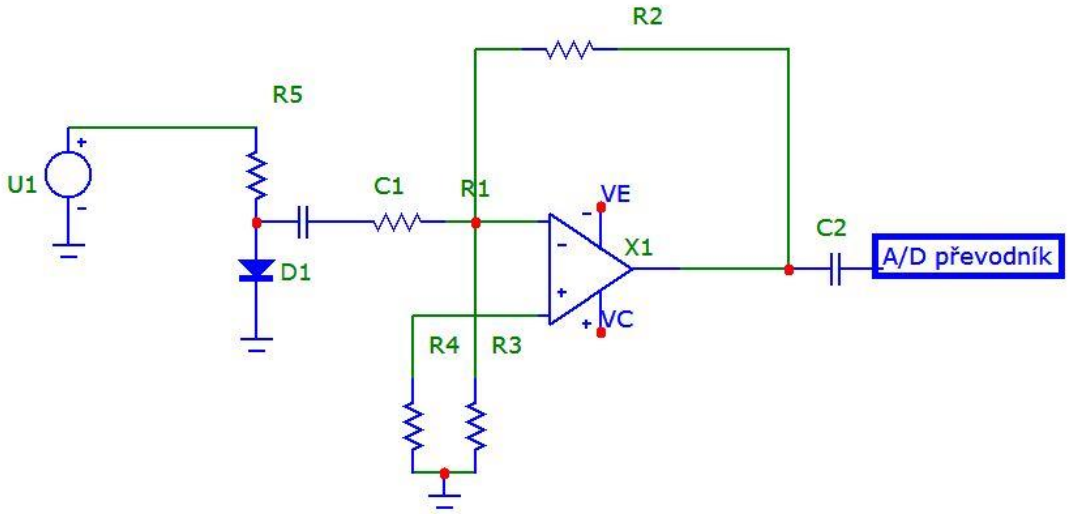


Figure 48. Ground Returns for Bias Currents with AC-Coupled Inputs

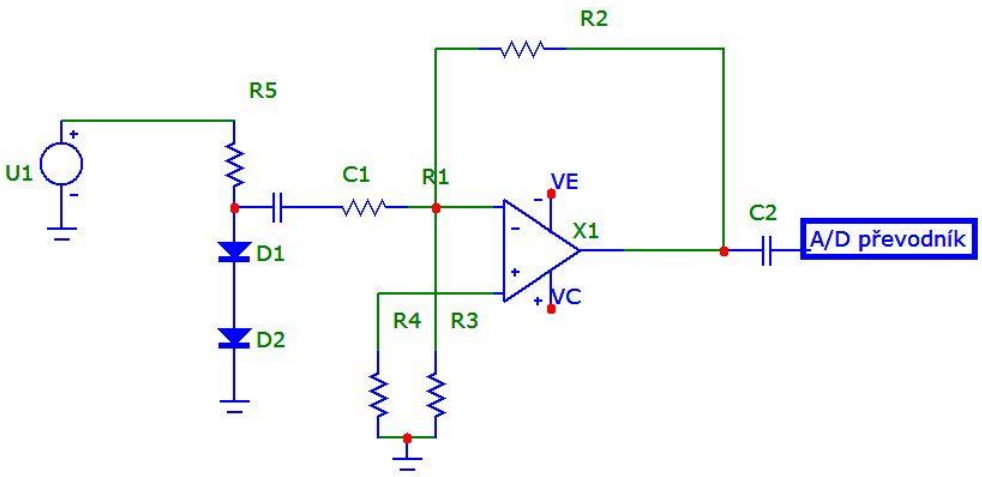
Obrázek 16 - Schéma zapojení přístrojového zesilovače [26]

Následující schéma znázorňuje kompletní zapojení s přístrojovým OZ, šumovou diodou a příslušnými odpory a kondenzátory:



Obrázek 17 - Schéma zapojení zesílení šumové diody 36NQ52 s přístrojovým zesilovačem AD620

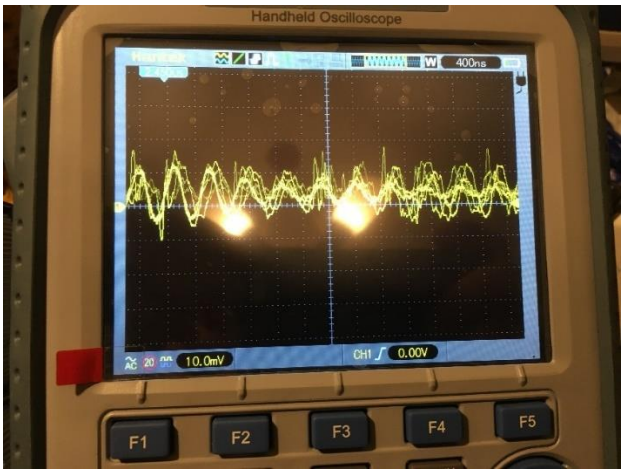
Při generování náhodných dat byla zkoušena i obyčejná LED místo šumové diody. Tato dioda relativně také dobře šumí, a proto byla i v jednom z pokusů začleněna do sériového zapojení se šumovou diodou, aby se ještě více zvýšila náhodnost generovaných dat.



Obrázek 18 - Schéma zapojení zesílení šumové diody 36NQ52 D1 v sériovém zapojení s LED D2

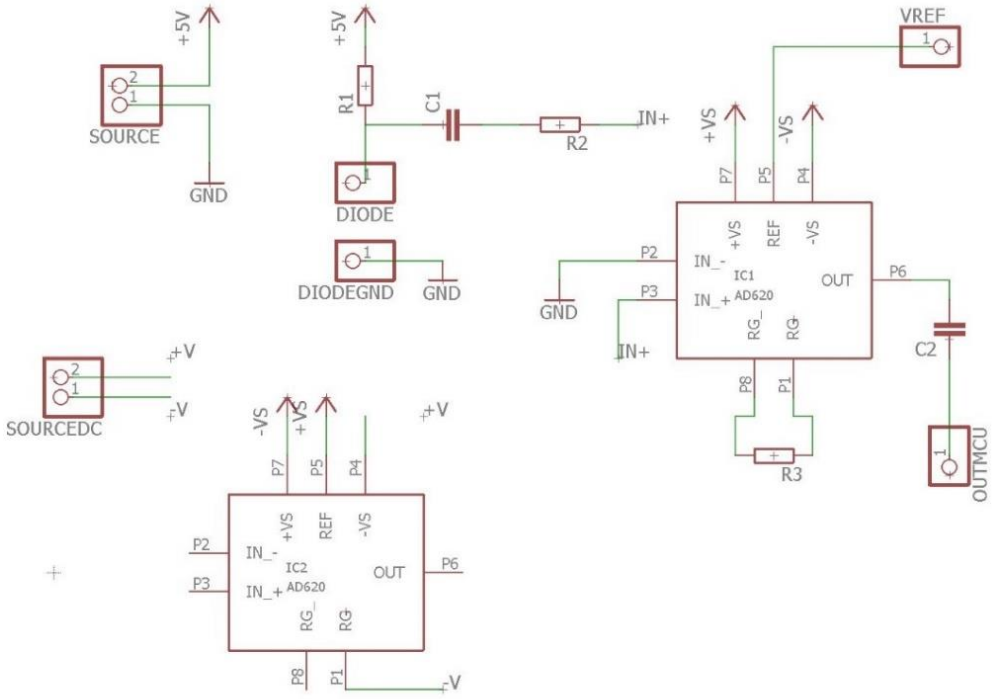
Nakonec po experimentech a měření bylo zvoleno zapojení pouze se šumovou diodou TESLA 36NQ52 a přístrojovým zesilovačem AD620.

Zařízení pro generování náhodného šumu pomocí šumové diody využívá hlavně blikavého šumu, který je opravdu náhodný a není závislý na žádné vstupní veličině. Vytvořený přípravek vytváří i ostatní druhy šumu, jako například tepelný a výstřelkový šum, které jsou ovšem minoritními šumy. Náhodnost výstupního napětí byla ověřena na osciloskopu.



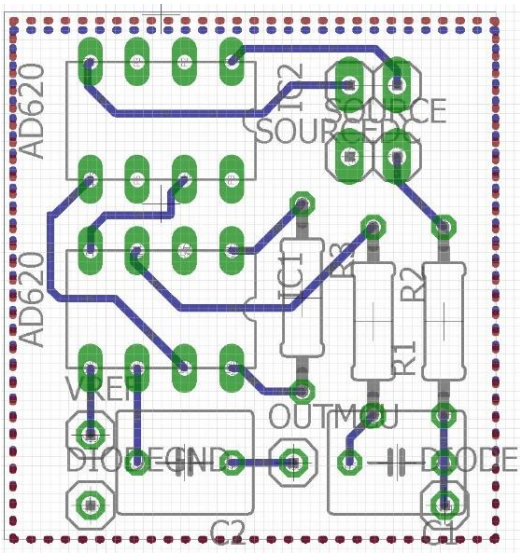
Obrázek 19 - Kontrola výstupu náhodného generátoru

Pro osazení součástek jsem vytvořil plošný spoj v návrhovém softwaru Eagle od firmy Autodesk. Pro plošný spoj bylo nutné nejprve vytvořit schéma propojů a také rozkreslit detailně součástky, které nebyly dostupné v knihovně programu. Jednalo se konkrétně o čip, který vytváří symetrická napájení ±5V. Výhodou ale bylo, že tato součástka je ve standardním pouzdru a tak jsem jen přepracoval stávající součástku z knihovny.



Obrázek 20 - Schéma propojení desky plošných spojů

Po vytvoření schématu, jsem mohl pokročit k tvorbě plošného spoje.



Obrázek 21 - Deska plošných spojů

Po dokončení celého návrhu byla data odeslána do výroby firmy PragoBoard s.r.o.. Do výroby je potřeba zaslat data do v definovaných formátech a specifikacích uvedených na stránkách firmy. Pro výrobu desky plošných spojů je potřeba například označení počtu vrstev desky plošného spoje, materiálu pro výrobu desek, detailní výkresy jednotlivých vrstev a podobně. Detailně jsou tyto požadavky dostupné na webových stránkách PragoBoardu [27].

7.4 Návrh způsobu napájení

Při návrhu zapojení pro náhodné generování šumu v reálném čase jsem provedl hrubý odhad výpočtu teoretické spotřeby. Toto počítání jsem provedl ještě před nákupem součástek, a proto jsem zvolil průměrnou spotřebu polovodičové diody, která činí cca. 10mA. Reálnou spotřebu u šumové diody jsem nikde nenalezl a ani se mi ji nepovedlo různými metodami určit přesněji. Použitá šumová dioda má při měření průchodu proudu nestálý charakter. Hodnota spotřebovávaného proudu se pohybovala mezi 6 - 12mA. Je nutné, aby zařízení bylo nezávislé na elektrické síti, a tedy musí být provozuschopné z baterie. Při zvolení kvalitní Lithium-iontové baterie, která se například umisťuje do tabletů jsme schopni se dostat na kapacitu baterie okolo hodnoty 4000-5000mAh při napětí 3,7V. Tuto kapacitu baterie ale nemůžeme využít na 100%,

jinak by se baterie zničila. Je proto potřeba baterii využít s rezervou. Pro 3,7V a spotřebu okolo 10mA se dostáváme na cca. 500h nepřetržitého provozu na tuto baterii tak, aby nedošlo k jejímu porušení. Provoz na baterii by vystačil na něco málo přes 20 dní. Toto je sice hrubý odhad, ale v porovnání se spotřebou mikroprocesoru je odhadovaná spotřeba generátoru náhodného šumu příliš vysoká. Byla tedy zvolena taková varianta, že jednou za delší dobu proběhne nahrání nových dat do paměti za pomoci uživatele. V normálním pracovním režimu zařízení data načítá z předem uložených vygenerovaných dat pomocí atmosférického šumu a tato data kombinuje s daty načtenými z analogově digitálního převodníku. Zařízení je vytvářeno jako experiment a tedy si můžeme, pokud to bude možné, dovolit zapojit zařízení do elektrické sítě. Pokud bude možné zařízení zapojit do elektrické sítě nebo k němu umístit větší baterii, pak bude zařízení možno provozovat v režimu generování náhodných dat v reálném čase pomocí šumové diody.

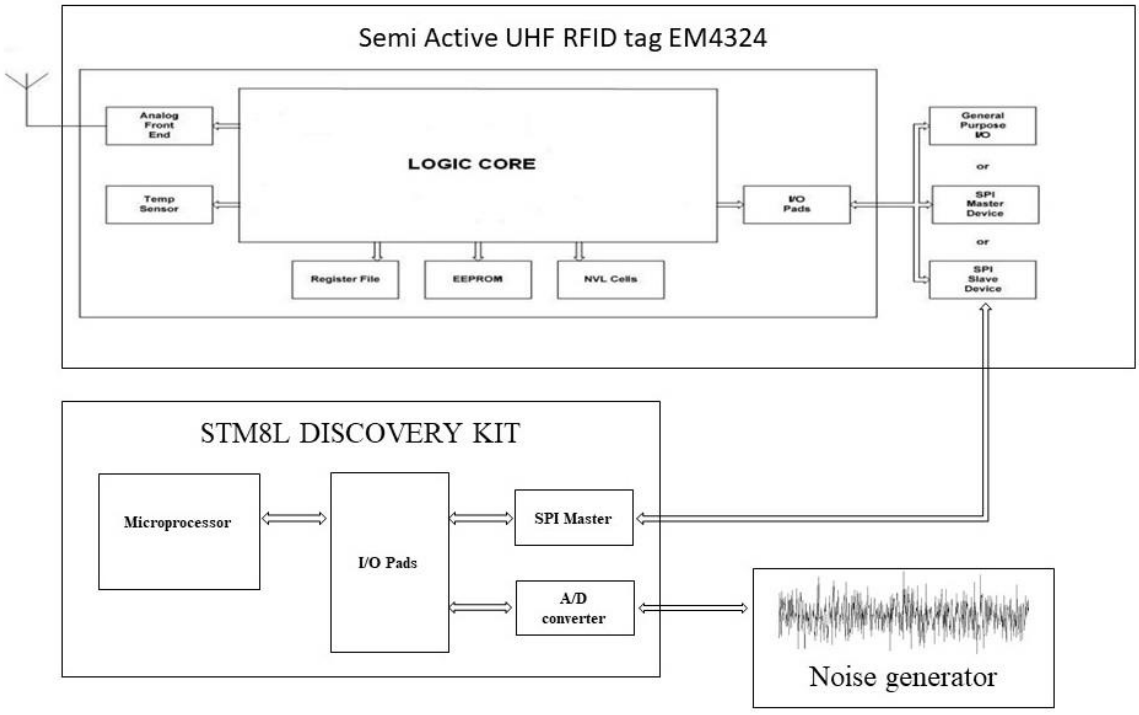
7.5 Semiaktivní RFID UHF tag EM4324

Po vytvoření opravdu náhodných dat se data mohou zasílat do zařízení, které bude náhodná generovaná data vysílat pomocí radiových vln do okolí. Jak již bylo zmíněno v úvodu kapitoly 7 - Návrh zařízení byl zvolen semiaktivní RFID UHF tag od firmy EM Microelectronic EM4324. Tento tag byl zvolen hlavně proto, že má k dispozici SPI rozhraní.

Zvolené zařízení od EM Microelektronic je semiaktivní širokopásmový UHF RFID tag. Je kompatibilní s normou EPCglobal druhé generace a také s normou ISO 18000-6C. RFID tag má vylepšenou verzi sady funkcí EPC+, která má lepší a rychlejší zpracování dat, než sada funkcí EPC druhé generace. Zařízení je přizpůsobeno a dimenzováno pro používání v drsných podmínkách. Samo zařízení i dodávaná baterie vydrží veliký rozsah teplot od -40°C do 85°C. Zařízení EM4324 obsahuje i integrovaný teploměr, který hlídá rozpětí teplot a při vyšších teplotách zařízení zasílá alarm uživateli při čtení dat nebo se automaticky vypíná, aby nedošlo k jeho poškození. Teploměr je možné využít i pro uživatelské aplikace, kdy si společně s informacemi uloženými v zařízení přečteme i aktuální okolní teplotu. Při výrobě čipu byl kladen důraz na funkčnost v přítomnosti vody nebo kovu. Na zařízení se nachází čtyřbitová sběrnice. Čtyřbitová sběrnice může být konfigurována jako sběrnice SPI nebo jako

vstupně/výstupní svorky pro čtyři diskrétní signály. V tomto případě je zvolena možnost SPI sběrnice. Sběrnice je nastavena jako SPI slave. SPI master je nastaven na mikroprocesor s A/D převodníkem. Zařízení má integrovanou správu napájení. Správa napájení slouží k prodloužení životnosti a výdrže baterie. Při vybití nebo poškození baterie umí zařízení pracovat v pasivním režimu. Zařízení má také integrovanou EEPROM paměť, do které se můžou data ukládat v průběhu zpracování informací. Pokud uživatel hlídá prostřednictvím RFID tagu nějaké události, pak nemusí číst data z RFID tagu neustále, ale stačí tato data přečíst jednou za čas. Uživatel si přečte data uložená přímo z EEPROM paměti. Do zařízení je možno nahrát i jednodušší programy pro zpracování dat ze sběrnice.

Způsob propojení semiaktivního RFID UHF tagu s mikroprocesorem a generátorem náhodných dat je uveden na následujícím blokovém schématu:



Obrázek 22 - Blokové schéma propojení UHG tagu s generátorem náhodných čísel [28]

7.6 Popis obsluhy a funkce zařízení pro generování náhodných dat

Zařízení se skládá ze dvou dílů. Oba díly mohou být napájené z baterie nebo z elektrické sítě. K napájení z baterií je k dispozici přípravek pro stabilizaci napětí. První díl obsahuje procesor osazený na vývojovém kitu STM8L Discovery. Tento díl se připojuje k semiaktivnímu RFID tagu pomocí čtyř vodičů, po kterých probíhá komunikace sběrnicí SPI. Tento díl je velice úsporný z hlediska spotřeby energie a je schopný pracovat pouze sám o sobě. Tento díl je možné provozovat dlouhou dobu na baterii. V tomto režimu zařízení pracuje s daty v paměti, která jsou ve výchozím nastavení systému vygenerována pomocí atmosférického šumu. Tato data jsou generována na webové stránce www.random.org, kde je aplikace pro generování opravdu náhodných dat a každá generovaná posloupnost zde projde testem na náhodnost dat. V tomto režimu je na displeji zobrazen symbol „M“ – Memory (paměť), kdy jsou data zpracovávána v paměti zařízení. Tato data se před odesláním do semiaktivního RFID tagu upravují matematickými operacemi. Provádím na nich operaci Exkluzivní disjunkce a součtu s využitím předchozích dat a nezatíženého vstupu na Analogově digitálním převodníku. Data z Analogově digitálního převodníku jsou závislá na okolních podmínkách a generují data s pseudonáhodnou posloupností. Tato pseudonáhodná posloupnost je použita k modifikaci nahrané opravdu náhodné posloupnosti dat. Těmito matematickými úpravami zvýším počet opravdu náhodných dat, kterých se do paměti mikroprocesoru příliš mnoho nevejde. Touto úpravou zvýším nezávislost generovaných a zmenším pravděpodobnost odposlechu uložených dat. Úpravy dat popisuje následující vzorec:

$$Y[i] = \{(Y[i-6])\ XOR\ (X[i])\} + \{Y[i-3]\}, \text{ kde} \qquad (7.1)$$

Y[i] jsou náhodná data uložená na i-té pozici v sekvenci náhodných dat v paměti a zároveň jsou tato data na výstupu do semiaktivního RFID tagu

Y[i-6] jsou náhodná data uložená před 6-ti kroky do sekvence náhodných dat v paměti

Y[i-3] jsou náhodná data uložená před 3-mi kroky do sekvence náhodných dat v paměti

X[i] jsou náhodná data načtená pomocí nezatíženého vstupu Analogově digitálního převodníku procesoru

XOR je matematická operace nazývaná exkluzivní disjunkce. Tato funkce se používá velmi často v kryptografii. Využívají jí například šifry typu DES, AES a i některé verze hašovacích funkcí.

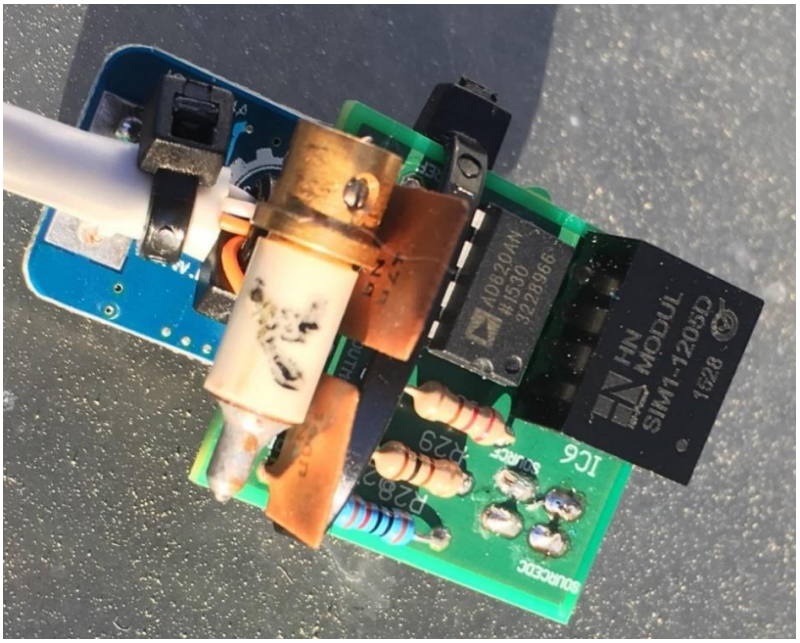
Pravdivostní tabulka funkce XOR:

B	**A**	**A** *XOR* **B**
0	0	0
0	1	1
1	0	1
1	1	0

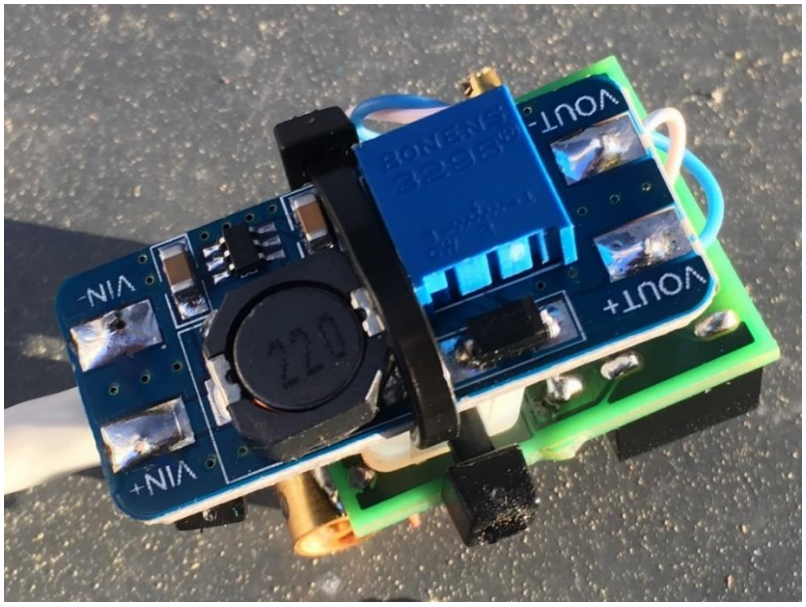
Při použití pouze první části zařízení hrozí po delší době opakování dat. Proto byla vytvořena druhá část, kterou lze připojit k mikroprocesoru. Druhá část je rozšiřitelným doplňkem k nízkopříkonovému procesoru. Po připojení tohoto příslušenství klesá doba běhu zařízení na baterii. Celé zařízení pro generování opravdu náhodných dat spotřebovává proud o velikosti přibližně 32 mA. Generátor opravdu náhodných dat je realizován šumovou diodou TESLA 36NQ52 a operačním zesilovačem AD620. Generátor náhodných dat obsahuje i regulovatelný Step up měnič pro napájení z různých druhů baterií či zdrojů. Ve výchozí konfiguraci je zařízení nastaveno pro napájení z 5V výstupu mikroprocesoru. Zařízení se připojí k vývojové desce STM8L Discovery, která sama pozná připojené příslušenství a začne odesílat do semiaktivního RFID tagu opravdu náhodná data, generovaná pomocí připojeného příslušenství pro generování opravdu náhodných dat. Po připojení příslušenství se na displeji změní symbol „M“ – Memory (paměť) na symbol „R“ – Random (náhodný generátor). Po připojení příslušenství se přepíší nahraná data v procesoru na nově vygenerovaná data. Algoritmus změny dat je shodný s předchozím případem s jediným rozdílem, kdy nebereme náhodná data z nezatíženého analogově digitálního převodníku, ale z náhodného generátoru dat se šumovou diodou připojeného na analogově digitální převodník.

$$Y[i] = \{(Y[i-6])\ XOR\ (Z[i])\} + \{Y[i-3]\}, \text{ kde} \qquad (7.2)$$

Z[i] jsou náhodně generovaná data pomocí připojeného generátor opravdu náhodných dat na vstupu analogově digitálního převodníku procesor.



Obrázek 23 - Realizovaný Hardwarový generátor opravdu náhodných čísel



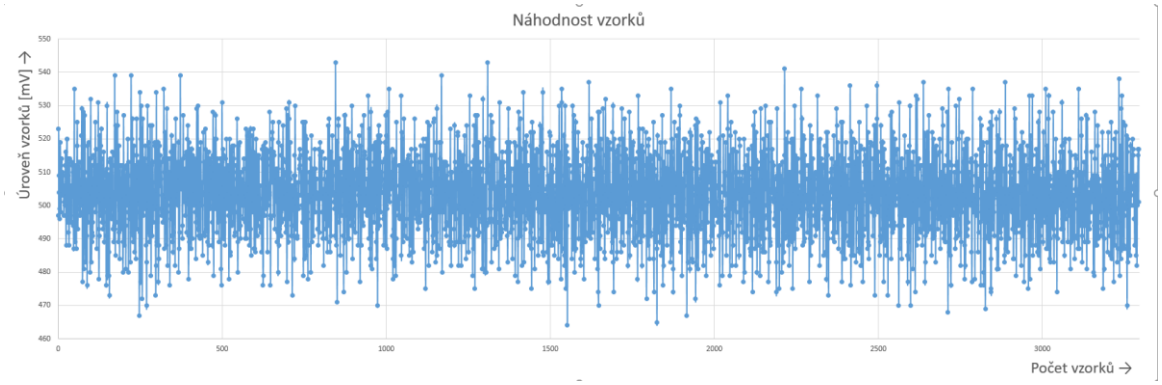
Obrázek 24 - Regulovatelný Step up měnič pro generátor náhodných čísel

8 Test náhodnosti dat

Po sestrojení zařízení jsem provedl test náhodnosti dat. Provedený test náhodnosti generovaných dat proběhl úspěšněji, než jsem předpokládal. Provedl jsem 8x sérii testů náhodnosti dat. Při testování byly různě měněny jak parametry testů, tak vstupní data. Používal jsem testovací sadu NIST. Tato sada je primárně určená pro velmi velké soubory s mnoha náhodnými daty.

Mikroprocesor, který zpracovává data je pouze 8mi bitový a má malou paměť. Do jeho paměti je tedy možné umístit jen velmi omezené množství dat. Z těchto důvodů jsem šel cestou nahrání dat do počítače z generátoru náhodných čísel pomocí do digitálního voltmetru s USB výstupem. Následně jsem chtěl otestovat náhodnost vygenerovaných dat testovací sadou NIST. Tímto způsobem nebyl naměřen žádný šum. Problém byl na straně digitálního voltmetru. Digitální voltmetr měřená data průměruje, a tak odstraňuje veškerý šum. Tento problém byl vyřešen pomocí A/D převodníku, který data z analogové roviny převede do roviny digitální. Vzorky byly nahrány pomocí STM8L Discovery kitu, který je součástí mého výrobku a v tomto testu komunikoval prostřednictvím SPI s jiným mikroprocesorem. Tento mikroprocesor umí komunikovat pomocí USB s počítačem a zobrazovat přijímaná data prostřednictvím virtuálního sériového displeje. Díky tomuto způsobu nahrání dat do počítače jsem měl k dispozici přibližně 10x více dat, než se vejde do mikroprocesoru. Tímto způsobem jsem nahrál soubor s 3296-ti náhodnými vzorky. I takto velké množství dat bylo pro skupinu testů náhodnosti dat nedostatečné. Bylo by možné načíst potřebné množství dat, kde ale narážím na další problém, a to konkrétně u načítání dat do počítače. Způsob, jakým načítám data do počítače, neumožňuje měnit formát výstupních dat. Tato načtená data jsou v dekadickém formátu a musí se v počítači převést do binární soustavy, kterou vyžaduje testovací program. Převod do binární soustavy není jedinou překážkou. Další překážkou je úprava formátu oddělování jednotlivých čísel. Po načtení jsou data ve sloupci. Program vyžaduje data v řádcích a oddělená určitými značkami. Po sériích úprav jsem zjistil, že je nejjednodušší data vložit do Excelu, kde si je převedu na binární čísla a transponuji stávající matici velikosti 3296 řádků a 1 sloupec na matici 1 řádek a 3296 sloupců. Následně jsem data přenesl do Wordu. Word má integrovanou funkci nahrazení

znaků. Tuto funkci jsem využil pro nahrazení tabulátorů mezi jednotlivými znaky mřížkou. V tomto bodě se vyskytlo největší úskalí. Počítač, který jsem využil na tyto úpravy, není zrovna nevýkonný stroj, a i tak měl problémy s prohledáním takto velké matice a nahrazením symbolů jedniček a nul následovaných mezerou vytvořenou pomocí tabulátoru za jedničky a nuly následované mřížkou. Takto upravená data jsem překopíroval do textového souboru, který měl již správný formát. Aplikace již tento správný datový soubor podporuje. Z hlediska dat v paměti mám již dostupná data přibližně 10x větší, než je dostupná paměť v použitém procesoru pro načítání dat a proto považuji tento vzorek za dostatečný. Nemohl jsem tedy vykonat všech 15 dostupných subtestů. U čtyř subtestů mi testovací sada NIST sdělila, že mám příliš malý počet dostupných dat. Program pro tyty čtyři subtesty potřebuje řádově MB dat. Moje data mají velikost přibližně 43kB. V doporučení se i uvádí, že tyto subtesty jsou detailní a podrobné testy velkých souborů dat. Při 8-mi sériích testů s různými nastaveními vyšly testy relativně stabilně se shodným výsledkem. Data jsou dle těchto testů náhodná.



Obrázek 25-Náhodný naměřený šum generovaný šumovou diodou TESLA 36NQ52

Zde přikládám ukázky výsledků z jedné série testů, kde je vidět i příklad testu, který byl vyhodnocen jako neúspěšný.

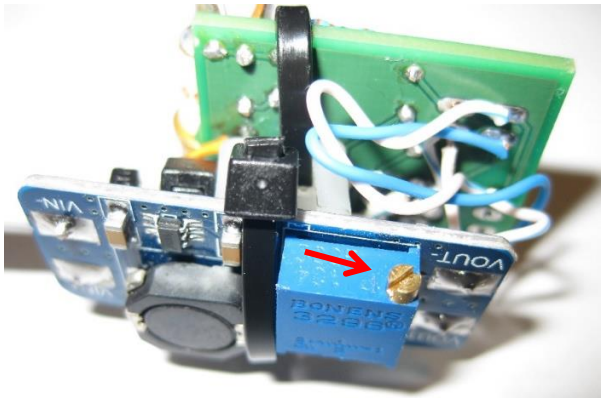
```
                    FREQUENCY TEST
-----------------------------------------------
COMPUTATIONAL INFORMATION:
-----------------------------------------------
(a) The nth partial sum = 4
(b) S_n/n               = 0,4
-----------------------------------------------
SUCCESS                 p_value = 0,205903210732068

                        BLOCK FREQUENCY TEST
```

```
                    ---------------------------------------------
                    COMPUTATIONAL INFORMATION:
                    ---------------------------------------------
                    (a) Chi^2          = 1,6
                    (b) # of substrings = 1
                    (c) block length    = 10
                    (d) Note: 0 bits were discarded.
                    ---------------------------------------------
SUCCESS                      p_value = 0,205903210732068

                                    RUNS TEST
                    ---------------------------------------------
                    COMPUTATIONAL INFORMATION:
                    ---------------------------------------------
                    (a) Pi                    = 0,7
                    (b) V_n_obs (Total # of runs) = 3
                    (c) V_n_obs - 2 n pi (1-pi)                2 sqrt(2n) pi (1-pi)
                    ---------------------------------------------
SUCCESS                      p_value = 0,366256395824783

                                                        LONGEST RUNS OF ONES TEST

                    ---------------------------------------------

                    COMPUTATIONAL INFORMATION:

                    ---------------------------------------------

                    (a) N (# of substrings)  = 125
                    (b) M (Substring Length) = 8
                    (c) Chi^2                = 323,318330568578
                    ---------------------------------------------

                        F R E Q U E N C Y

                    ---------------------------------------------

                     <=1    2    3    >=4   P-value  Assignment
                    0 5 19 101
FAILURE
```

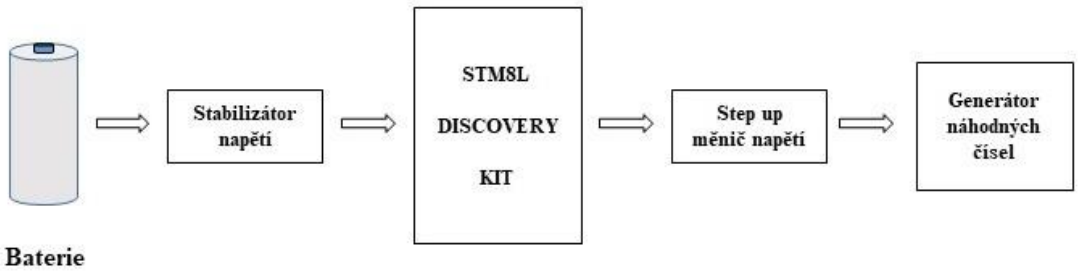
9 Zhodnocení vytvořeného zařízení

K problematice popisované v této diplomové práci bylo vytvořeno zařízení, které generuje opravdu náhodná data. Tato náhodná data jsou generována pomocí šumové diody TESLA 36NQ52 a zesílena operačním zesilovačem AD620. Náhodnost dat byla ověřena pomocí testovací sady NIST. Testovací sada je standardizována americkým úřadem pro standardy a technologie NIST. Generovaná data jsou digitalizovaná procesorem STM8L152C6 využitím integrovaného analogově digitálního převodníku. Data jsou následně zpracována ve zmíněném procesoru a zasílána po SPI sběrnici do semiaktivního RFID UHF tagu. Generátor náhodných čísel má vyšší spotřebu, a proto je program, který běží v procesoru rozdělen na 2 režimy. První režim je režim provozu na baterii s dlouhou dobou výdrže. V tomto režimu je aktivní pouze mikroprocesor, který má nahraná data v paměti a tato data jsou dále upravována pomocí nezatíženého vstupu analogově digitálního převodníku na mikroprocesoru. Takto vytvořená data se odesílají do semiaktivního RFID UHF tagu. Pokud zařízení běží v tomto režimu na baterii, pak daný uživatel musí počítat s tím, že jsou generovaná data pouze pseudonáhodná a jejich náhodnost je zvýšena pomocí nezatíženého vstupu analogově digitálního převodníku. Data generovaná tímto způsobem nejsou opravdu náhodná a mohou se za určitou dobu opakovat. Druhý režim předpokládá napájení ze síťového rozvodu nebo z baterie s vyšší kapacitou. Program generuje opravdu náhodná data a odesílá je v reálném čase do semiaktivního RFID tagu. Tento režim nevylučuje běh na baterii, ale uživatel musí počítat s nižší výdrží celého zařízení. Jelikož je tento přípravek konstruován hlavně jako experiment, pak si napájení ze síťového rozvodu můžeme dovolit. Jako další vylepšení zařízení bych doporučoval použít jiný nízkopříkonový procesor, který by měl větší paměť, na kterou by bylo možné nahrát několikanásobně více náhodných dat dopředu a paměť by byla typu Flash nebo jiného druhu, který udrží informace i po vypnutí napájení. Paměť by mohla být realizována i připojenou paměťovou kartou. Další možností, jak zlepšit tuto aplikaci je vývoj správy napájení, kdy by byl mikroprocesor schopný spínat náhodný generátor automaticky po vyčtení náhodných dat.

Obě zařízení je možné napájet za pomoci stabilizátoru napětí z jakékoli baterie. Základní nastavení zařízení je pro baterie či bateriové články v sérii, které mají vyšší napájecí napětí jak 5V. Zařízení s mikroprocesorem je konstruováno s ohledem na využití baterií i nižšího napájecího napětí 3,3V. Při této konfiguraci a potřebě napájení z tohoto zdroje i generátoru náhodných čísel je zapotřebí změnit nastavení Step up měniče u generátoru náhodných čísel. Změna se provádí potenciometrem na hraně Step up měniče.



Obrázek 26 - Změna úrovně napájení pro generátor náhodných čísel



Obrázek 27 - Blokové schéma napájení

Napájení bylo řešeno pouze u zařízení pro generování náhodných čísel a jeho zpracování. RFID UHF tag má své řešení napájení z baterie. Napájení může být realizováno i 5V zdrojem ze zásuvky. Zdroj z elektrické sítě nebo vlastní baterie se stabilizátorem napětí se připojí na pin s označením 5V a GND umístěný vývojové desce STM8L DISCOVERY. Z desky STM se z 5V rozvodu napájí generátor náhodných čísel. Je nutné připojit rovněž pin GND. V případě nutnosti lze obě zařízení napájet vlastním akumulátorem.

10 Závěr

Cílem této diplomové práce bylo vytvořit Semiaktivní RFID UHF tag s generátorem náhodných čísel respektující standard GS1 EPC GEN2. Ke splnění tohoto cíle jsem potřeboval prostudovat problematiku realizace hardwarových generátorů náhodných čísel použitelných pro nízkopříkonové aplikace. Následně tento hardwarový generátor náhodných čísel zkonstruovat a propojit se semiaktivním UHF RFID tagem. Dalším cílem práce bylo náhodná data vygenerovaná hardwarovým generátorem náhodných dat ověřit v testu kvality náhodných dat.

Součástí vypracování diplomové práce je potřebná teorie pro návrh a realizaci zařízení. V teoretické části je popsaná technologie RFID, typy náhodných generátorů včetně jejich klasifikace a analýzy. Je zde také popsáno využití RFID technologie v Internetu věcí, druhy kryptografie a praktický návrh zařízení.

Vytvořené zařízení generuje náhodná data a následně je zasílá po SPI sběrnici do semiaktivního RFID UHF tagu. SPI je teoreticky navržené v programu pro mikrokontrolér, jen zatím nebylo z časových důvodů implementováno. Ukázka implementace SPI je uvedena v kapitole 12 - Přílohy. SPI nebylo zatím implementováno, protože jsem se při návrhu zařízení věnoval hlavně kvalitnímu zpracování generování opravdu náhodných a pseudonáhodných dat. Problémy s komunikací po SPI sběrnici se v době odevzdávání diplomové práce snažím odstranit. Zařízení bude možné využít ke zvýšení zabezpečení u jakéhokoli RFID tagu, který má komunikační rozhraní SPI. Zařízení má dva režimy provozu. Jednou z možností je režim, který je primárně určen pro běh systému na baterii. U tohoto režimu máme velmi nízkou spotřebu. U provozu na baterii je nevýhodou, že nemáme zajištěna opravdu náhodná data. „Náhodná“ data zařízení generuje pomocí dat uložených v paměti. Data jsou následně kombinována pomocí nezatíženého vstupu analogově digitálního převodníku s předchozími stavy dat uložených v paměti. Pro mnoho aplikací tento způsob bude nejspíše dostatečný. Pokud by uživatel vyžadoval opravdu náhodná data, kde bude mít zaručeno, že se data nebudou nikdy opakovat, pak přichází na řadu druhý režim zapojení. Druhý režim pracuje na takovém principu, že se připojí hardwarový generátor opravdu náhodných dat k mikroprocesoru. Tato data jsou generována pomocí šumové diody TESLA 36NQ52, která se v minulosti využívala

v můstkových zapojeních pro ladění antén. Signál ze šumové diody je zesílen operačním zesilovačem AD620.

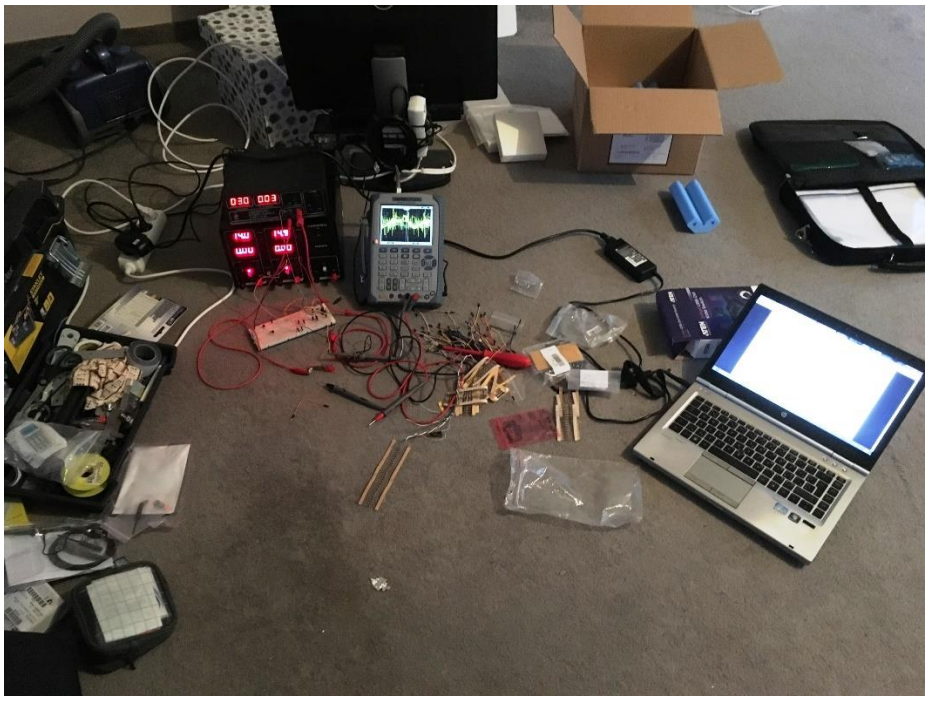
Zařízení s generátorem náhodných čísel poslouží jako zdroj náhodných dat dodávaných do semiaktivního RFID UHF tagu. Generovaná data se do semiaktivního RFID UHF tagu dodávají z důvodů zvýšení entropie dat. Zvýšení entropie dat napomáhá k zabezpečení RFID technologie. Zařízení dodává redundantní data semiaktivnímu RFID UHF tagu. RFID UHF tag vysílá svoje interní informace společně s náhodně generovanými daty. RFID UHF čtečka díky těmto redundantním informacím má již dostatek dat potřebných pro zabezpečení přenosu informace. Šifrovací algoritmus pro svou činnost potřebuje větší množství dat, která do systému dodáme náhodným generátorem.

Princip zvýšení zabezpečení je takový, že v prostoru bude vedle klasických semiaktivních RFID UHF tagů bez úpravy umístěn i jeden či více semiaktivních RFID UHF tagů s generátorem náhodných dat. Velikou výhodou této struktury rozmístění RFID technologie je nevýrazné zvýšení ceny celého systému. Přidaný RFID UHF tag s náhodným generátorem doplní redundantní informace k vysílaným informacím ostatních semiaktivních RFID UHF tagů. Díky doplnění redundantních informací k RFID datům uložených v tazích můžeme spolehlivěji zabezpečit data šifrovacími algoritmy, zejména od serveru middleware výše.. Tyto algoritmy pro svou činnost potřebují větší množství dat, které semiaktivní RFID UHF tagy bez úpravy nemají k dispozici.

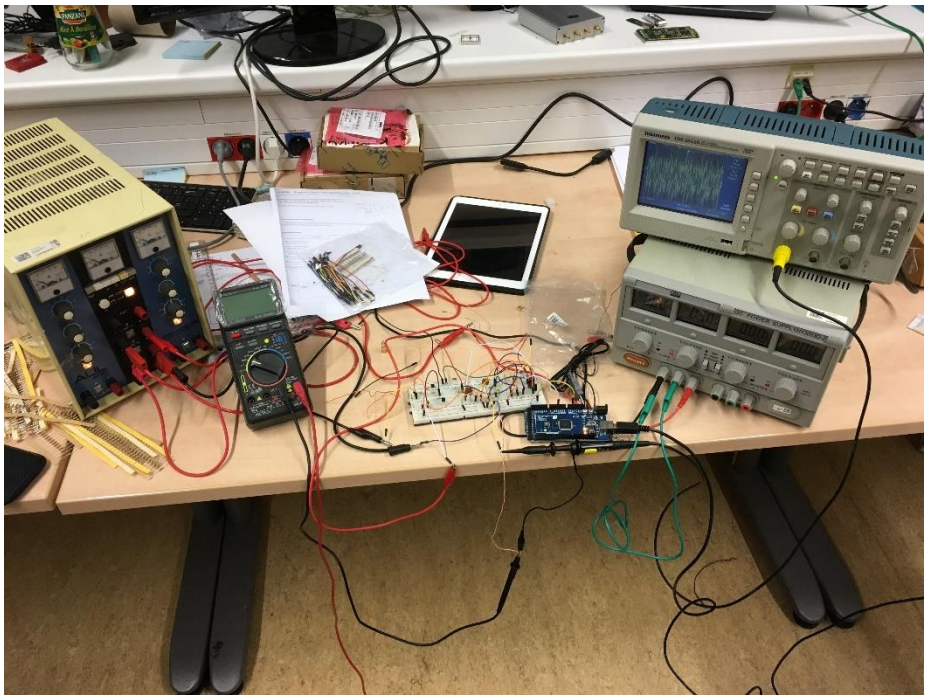
Během řešení a konstrukce jsem se setkal hlavně s problémy generování opravdu náhodných dat a se spotřebou celého zařízení. Generování opravdu náhodných dat je v digitálním světě problém. Opravdu náhodná data nelze generovat pouze softwarově. Vždy je zapotřebí hardwarový generátor využívající změnu některých přírodních měřitelných veličin. Přírodní veličiny nikdy nemívají periodický průběh, vždy je alespoň mírná odchylka od předchozího stavu. Problémem tedy zůstává pouze přesnost a správné rozlišení měření. K regulovanému generování dat za pomocí přírodních zdrojů a následné měření a načítání do digitálního světa je potřeba větší množství energie, než bylo v dané aplikaci na baterii, za podmínky dlouhé výdrže k dispozici. Z těchto důvodů je problematika generování náhodných dat rozdělena na dvě aplikace. Jedna z nich je generování opravdu náhodných dat a druhá je

generování pseudonáhodných dat, kde je náhodnost dat zvýšená kombinací s předchozími vzorky a nezatíženým vstupem analogově digitálního převodníku, který generuje další, méně závislou pseudonáhodnou posloupnost.

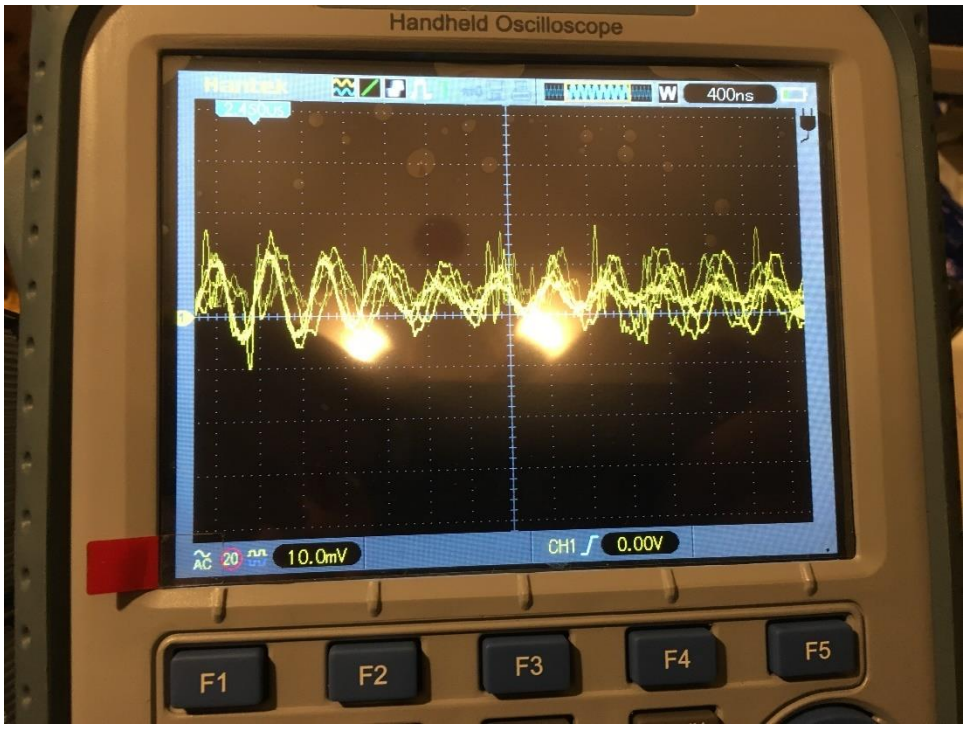
11 Fotodokumentace vývoje



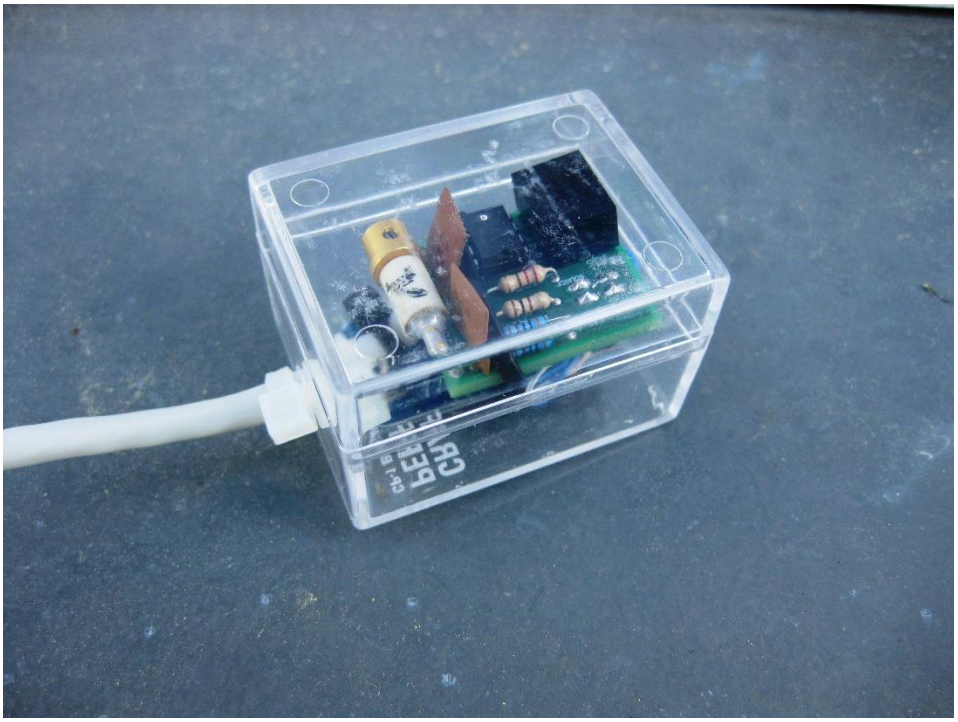
Obrázek 28 - První oživení šumové diody, zatím nestabilní šum



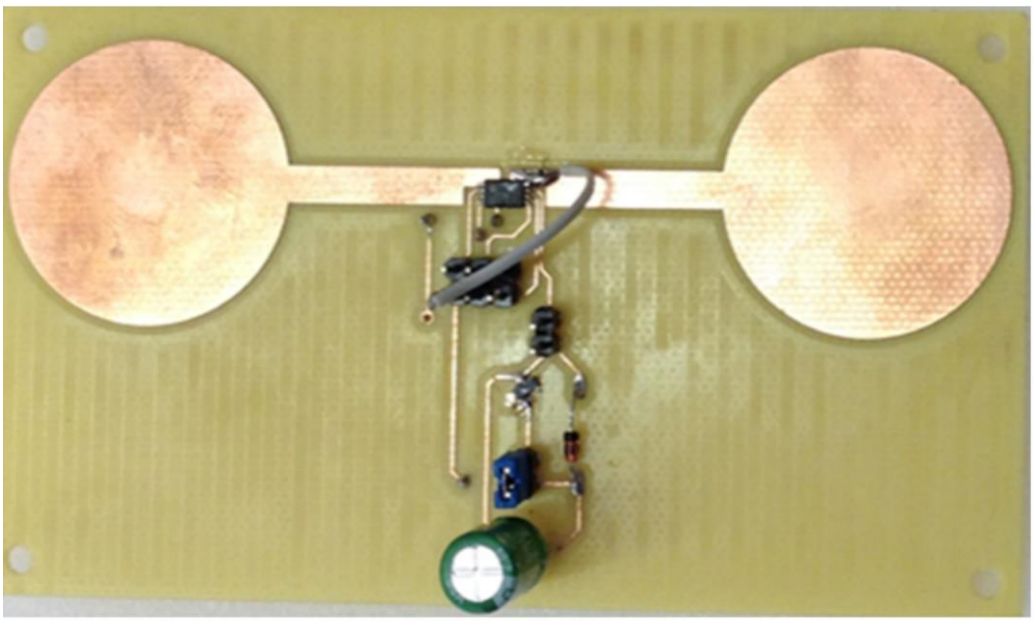
Obrázek 29 - Přidání přístrojového operačního zesílení pro stabilní šum



Obrázek 30 - Náhodný šum vyfocený na osciloskopu



Obrázek 31 - Mechanická ochrana generátoru náhodných dat proti poškození



Obrázek 32 - Semiaktivní RFID UHF tag navržený na katedře telekomunikací, fakulty elektrotechnické, ČVUT v Praze

12 Přílohy

```
//nastavení a deklarace SPI
#include "stm8l15x_spi.h"

SPI_TypeDef*      SPIx;

void SPI_Init(SPI_TypeDef* SPIx, SPI_FirstBit_TypeDef SPI_FirstBit,
          SPI_BaudRatePrescaler_TypeDef SPI_BaudRatePrescaler,
          SPI_Mode_TypeDef SPI_Mode, SPI_CPOL_TypeDef SPI_CPOL,
          SPI_CPHA_TypeDef SPI_CPHA, SPI_DirectionMode_TypeDef
          SPI_Data_Direction, SPI_NSS_TypeDef SPI_Master_Management,
          uint8_t CRCPolynomial);

//nastavení SPI výstupních a vstupích pinů pro SPI
GPIO_Init(GPIOC, GPIO_Pin_6, GPIO_Mode_Out_PP_Low_Fast);  //SCK - clock
GPIO_Init(GPIOC, GPIO_Pin_5, GPIO_Mode_Out_PP_Low_Fast);  //NSS - slave select
GPIO_Init(GPIOA, GPIO_Pin_2, GPIO_Mode_In_PU_No_IT);        //MISO
GPIO_Init(GPIOA, GPIO_Pin_3, GPIO_Mode_Out_PP_Low_Fast); //MOSI

CLK_PeripheralClockConfig(CLK_Peripheral_SPI1, ENABLE);
GPIO_ExternalPullUpConfig(GPIOC, (GPIO_Pin_7|GPIO_Pin_6|GPIO_Pin_5),ENABLE);
                SPI_Init(SPIx, SPI_FirstBit_MSB,
                                                SPI_BaudRatePrescaler_2,
                                                SPI_Mode_Master, SPI_CPOL_Low,
                                                SPI_CPHA_1Edge,
SPI_Direction_2Lines_FullDuplex,SPI_NSS_Soft,SPI_CRC_RX);
          SPI_Cmd(SPIx,ENABLE);
SPI_SendData(SPIx, pole_hodnot[i]);  //odesilani dat po SPI
```

Příloha 1 – ukázky nastavení SPI komunikace

13 Reference

[1] *Od radarů protivzdušné obrany k ochraně zboží* [online]. b.r. [cit. 2017]. Dostupné z: https://www.rfid-epc.cz/co-je-rfid/historie-rfid#collapse-text--accordion-0

[2] ING. BC. LUKÁŠ VOJTĚCH, Ph.D. *Vysokoškolské přednášky předmětu Bezdrátové technologie a senzorové sítě*. Praha: ČVUT FEL, Praha, 2017.

[3] ING. BC. LUKÁŠ VOJTĚCH, Ph.D. *Access server FEL ČVUT* [online]. 2009 [cit. 2017]. Dostupné z: http://access.fel.cvut.cz/view.php?cisloclanku=2009020001

[4] *ITBIZ* [online]. 2007 [cit. 2017]. Dostupné z: http://www.itbiz.cz/rfid-bezpecnost

[5] *ETSI World Class Standards* [online]. b.r. [cit. 2017]. Dostupné z: http://www.etsi.org/technologies-clusters/technologies/radio/rfid

[6] ÚŘAD, Český. *Využívání vymezených rádiových kmitočtů* [online]. b.r. [cit. 2017]. Dostupné z: http://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu

[7] ÚŘAD, Český. *Informace ze seminářů ČTÚ pro provozovatele WiFi sítí (RLAN) a zařízení* [online]. b.r. [cit. 2017]. Dostupné z: http://www.ctu.cz/informace-o-seminarich-ctu-pro-provozovatele-wifi-siti-rlan-zarizeni

[8] RFID PORTAL. *Základní informace o technologii RFID* [online]. b.r. [cit. 2017]. Dostupné z: http://www.rfidportal.cz/index.php?page=rfid_obecne

[9] REPUBLIC, GS1. b.r. [cit. 2017]. Dostupné z: http://www.gs1cz.org/epc-rfid/

[10] GS1, . *EPC Tag Data Standard - Release 1.10* [online]. 2017 [cit. 2017]. Dostupné z: http://www.gs1.org/sites/default/files/docs/epc/GS1_EPC_TDS_i1_10.pdf

[11] HAAHR, Dr. *Introduction to Randomness and Random Numbers* [online]. b.r. [cit. 2017]. Dostupné z: https://www.random.org/randomness/

[12] ZOUHAR, Bc. *Generátor náhodných čísel - diplomová práce*. Brno: VUT v Brně, 2010.

[13] ANDREW RUKHIN, Juan. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications* [online]. 2010 [cit. 2017]. Dostupné z: http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

[14] KLÍMA, Vlastimil. *Statistické testy NIST*. 2010, s. 16.

[15] KUKKO, MARCEL. *ENTROPICKÝ GENERÁTOR NÁHODNÝCH ČÍSEL - Bakalářská práce* [online]. 2014 [cit. 2017]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=85262

[16] PETRŽELA, Jiří. *Analýza šumu v elektronických obvodech* [online]. b.r. [cit. 2017]. Dostupné z: http://www.urel.feec.vutbr.cz/MTEO/mteo/sumy.pdf

[17] DOBEŠ, Josef. *Šumová analýza* [online]. Praha: ČVUT FEL, 2013 [cit. 2017]. Dostupné z: http://radio.feld.cvut.cz/personal/dobes2/Noise.pdf

[18] MODERÁTOR: JAN BUMBA, host:. *Český rozhlas - archiv* [online]. 2016 [cit. 2017]. Dostupné z: http://prehravac.rozhlas.cz/audio/3607275

[19] ING. TOMÁŠ VANĚK, Ph.D. *Vysokoškolské přednášky předmětu Informační bezpečnost*. Praha: ČVUT-FEL, 2016.

[20] ALFRED J. MENEZES, Paul. *Applied Cryptography*. CRC Press, 1996.

[21] MURRAY, Kevin. *Scytale - Ancient Spy Gadget - Early Tweet* [online]. 2014 [cit. 2017]. Dostupné z: https://spybusters.blogspot.cz/2014/07/scytale-ancient-spy-gadget-early-tweet.html

[22] VALENTINE, VOJTECH,. Design of Solar Harvested Semi Active RFID. *Dspace.vsb.cz*. 2015.

[23] *STMicroelectronics*. b.r. Dostupné také z: http://www.st.com

[24] TESLA, . *Katalog diskrétních součástek TESLA*. b.r.

[25] *Šumový můstek* [online]. b.r. [cit. 30]. Dostupné z: http://www.cbdx.cz/clanek128-sumovy-mustek-1.htm

[26] *Datasheet Analog Devices AD620* [online]. b.r. [cit. 2016]. Dostupné z: http://www.analog.com/media/en/technical-documentation/data-sheets/AD620.pdf

[27] *PragoBoard s.r.o.* b.r. Dostupné také z: www.pragoboard.cz/

[28] MICROELECTRONIC, EM. *Datasheet Semi Active UHF tag EM4324*. b.r.

14 Seznam obrázků