STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

ZABEZPEČENÁ KOMUNIKACE V NOVÝCH MODERNÍCH RÁDIOVÝCH SÍTÍCH

AUTOR Martin Frei

ŠKOLA Gymnázium Matyáše Lercha, Brno

KRAJ Jihomoravský

OBOR 18. Informatika

Brno 2018

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

ZABEZPEČENÁ KOMUNIKACE V NOVÝCH MODERNÍCH RÁDIOVÝCH SÍTÍCH

SECURE COMMUNICATION IN MODERN RADIO NETWORKS

AUTOR	Martin Frei
ŠKOLA	Gymnázium Matyáše Lercha, Brno
KRAJ	Jihomoravský
ŠKOLITEL	Ing. Radek Fujdiak, Ph.D.
OBOR	18. Informatika

Brno 2018

Prohlášení

Prohlašuji, že svou práci na téma Zabezpečená komunikace v nových moderních rádiových sítích jsem vypracoval samostatně pod vedením ing. Radka Fujdiaka, Ph.D. a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Dále prohlašuji, že tištěná i elektronická verze práce SOČ jsou shodné a nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých zákonů (autorský zákon) v platném znění.

V Brně dne 31. 1. 2018 Podpis:

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Poděkování

Děkuji svému školiteli ing. Radku Fujdiakovi, Ph.D. za hodiny konzultace, dostatek trpělivosti a hlavně pomoc při závěrečném psaní mé práce. Dále bych chtěl poděkovat všem, kteří mi odpovídali na mé dotazy ohledně řešené problematiky nebo poskytli jakoukoliv jinou pomoc.

Tato práce byla provedena za finanční podpory Jihomoravského kraje.

Anotace

Cílem této práce je vytvořit rychlé, bezpečné a nízkoenergetické E2E šifrování, které by doplnilo stávající absenci kryptosystému v nově rozrůstající se síti Sigfox a co nejlépe využilo již existujícího zabezpečení sítě.

Připojení k síti Sigfox dnes na celém světě využívá přes 727 milionů zařízení a je rozšířena ve 32 zemích včetně České republiky přesto síť postrádá ochranu důvěrnosti zpráv. Naše implementace šifry tento problém úspěšně řeší. Šifra je vhodná k vložení do každého zařízení využívající Sigfox, její použití razantně nenavýší energetickou náročnost a přidá uživateli tolik poptávané šifrování.

Klíčová slova

Internet věcí; šifrování; LPWAN; návrh a implementace zabezpečení; Sigfox; Vermanova dokonalá šifra;

Annotation

The goal of this research is to create fast, secure and low energy E2E encryption that would supplement the absence of such cryptosystem in the currently expanding Sigfox network and, at the same time, utilize the already existing network security as best as possible.

In spite of having more than 727 million devices worldwide and being extended in 32 countries including the Czech Republic, Sigfox lacks the protection of message confidentiality. Our system successfully solves this issue. It is suitable for any Sigfox device, its usage does barely increase the energy consumption and offers the, by users highly demanded, encryption.

Keywords

Internet of things; encryption; design and implementation of encryption; LPWAN; Sigfox; Verman cipher;

Obsah

Úvod

Sigfox je relativně novou rozrůstající se sítí, v ČR aktuálně pokrývá 92 % území a stále je rozšiřována (1). Jejími hlavními výhodami je velký dosah ve vnitřním i vnějším prostředí a nízká energetická náročnost, proto se implementuje do řady projektů ve městech, průmyslu, zdravotnictví, podnikání a také k ochraně majetku a přírody (2). Sigfox se dnes hojně využívá ve Francii, kde se pomocí zařízení připojených do sítě monitoruje tlak vody v požárních hydrantech (3), v Moskvě je k síti připojen systém chytrého parkování, který obsahuje přes 11000 senzorů (4). V Česku se zařízení připojená k síti Sigfox využívají jako GPS (Global Positioning System) trackery, pomáhající proti krádeži stromů. Již tyto příklady svědčí o možném obrovském budoucím rozvoji této sítě. Odhaduje se, že v roce 2020 bude objem trhu s IoT (Internet of Things) činit 267 mld. $ (5) a k síti bude připojeno přes 200 mld. zařízení (6).

Téma práce je zasazeno do atraktivní oblasti stále se rozvíjejícího Sigfoxu. Naším úkolem je navrhnout šifrování pro síť Sigfox a úspěšně ho implementovat do sestaveného vývojového kitu Arduino a tím vyřešit problém Sigfox s chybějící ochranou důvěrnosti. Budeme se zabývat problematikou distribuce klíčů, výběrem šifry samotné, zhodnotíme bezpečnostní rizika a provedeme rozsáhlá měření, která nám zaručí, že jsme vybrali správně. Každá šifra je bezpečná, ale jednotlivé implementace dané šifry už tak bezpečné být nemusí.

Před ukončením našeho výzkumu správci sítě implementovali do sítě Sigfox symetrické šifrování AES CTR (Advanced Encryption Standard Counter) (7), avšak toto šifrování není E2E (konec-konec z angl. End-to-End), nejsou o něm poskytnuty informace z hlediska jeho bezpečnosti, energetické náročnosti a navíc zprávy šifruje stejným klíčem, který se využívá pro HMAC (z angl. Keyed-hash Message Authentication Code).

Práce je rozdělena na 6 kapitol. První kapitola se zabývá krátkou definicí pojmu IoT (Internet of Things) a vysvětluje jeho význam. Druhá kapitola popisuje technologii LPWAN (Low-Power Wide Area Network) sítí a jejich využití v praxi. Třetí kapitola je věnována čistě síti Sigfox. Jsou zde popisovány základní parametry a architektura sítě, její výhody a nevýhody, předpoklady pro budoucí využití a hlavně je zde zhodnoceno její dosavadní zabezpečení. Kapitola čtvrtá je zasvěcena návrhu a výběru kryptografického systému, který v Sigfox chybí. Pátá kapitola se zabývá praktickou implementací vybrané šifry do zařízení, také je v ní popsán hardware, do kterého budeme šifrování implementovat. V poslední kapitole je šifra podrobena rozsáhlým měřením na odběr energie a rychlost šifrování. Tato měření mají dokazují, že jsme zvolili správně.

1 Internet of Things

Internet of Things (Internet věcí) poprvé definoval Kevin Ashton (Massachusetts Institute of Technology) (8), jako vzájemnou komunikaci všech věcí, které by měl někdo řídit. V roce 2013 ji definoval Bryce Barnes slovy: „*Je to chytré spojení chytrých zařízení, kterým se objekty mohou navzájem vnímat a komunikovat*“ (8). Dnes se již u nás IoT zapojuje do monitoringu vzdálených zařízení či objektů pomocí čidel. Do budoucna se plánuje implementace IoT i ve zdravotnictví. Například si představme malý senzor, který bude monitorovat naše fyzické zdraví a v případě nutnosti zavolá zdravotnickou službu. Internet věcí je poslední době na vzestupu, do jeho rozvoj, investuje řada technologických firem značné peníze (Google, Microsoft, T-Mobile a další).

Dnes se jeví IoT věcí jako dobrou alternativou pro M2M (Machine to Machine) (9), protože dokáže lépe řešit distribuci dat z čidel mezi jednotlivými pracovními stanicemi a přebírá spoustu užitečných prvků z M2M. Úplnou definici Internetu věcí nabízí práce (10).

2 LPWAN technologie

Výhodou LPWAN je nízká energetická náročnost a velký dosah. Dokáží pokrýt rozsáhlá území při menším počtu BTS oproti celulárním sítím druhé generace a vyšším (tzv. 2G+). Tyto vlastnosti jsou patrné již z jejich názvu. LPWAN sítě mají nízkou přenosovou rychlost, dokáží přenášet malý objem dat na velké vzdálenosti, proto jsou vhodné při distribuci informací z různých čidel. Sítě podporují obousměrnou komunikaci a více připojených zařízení než mobilní sítě. Provoz LPWAN je také mnohem ekonomičtější než dosavadní mobilní sítě. Obecný dosah zařízení s takovouto technologií se pohybuje se kolem 20 km, viz Tabulka 1 specifikace jednotlivých sítí (11).

Většina LPWAN sítí využívá bez licenční frekvenční spektrum, to eliminuje provozní náklady spojené s placením poplatků za využití licencovaného pásma, avšak používání na těchto frekvencích přináší také řadu omezení, jako nižší přenosová rychlost či rušení vnějšími vlivy. Řada zemí reguluje vyzářený výkon zařízení v daných pásmech. V Česku jsou LPWAN sítě regulovány Českým telekomunikačním úřadem (ČTÚ) (12). Přehled maximálního povoleného vyzářeného výkonu nám poskytne Tabulka 2 (11).

Technologie LPWAN sítí se dělí podle způsobu využití spektra na následující typy:

1. Využívá malé kanálové řetězce (Narrow Band, Narrow, Ultra Narrow Band) ke snížení šumu (13), hlavním představitelem u nás je Sigfox.
2. Mění přenosovou rychlost vzhledem k podmínkám v síti (SS, Spectrum) (14).

Technologii také rozdělujeme dle typu spektra:

1. Licenční například NB-IoT, Symphonylink,
2. nelicenční (ostatní).

2.1 Využití LPWAN technologií

Do budoucna je plánováno využití LPWAN technologie v digitalizaci mnoha odvětví našeho života. Tato odvětví bych rozdělil do několika částí (15):

- Smart Economy (optimalizace nákladů, pomoc firmám při monitoringu zboží),
- Smart Mobility (Systém sledování provozu, sdílení dopravních prostředků, inteligentní řízení dopravy, chytrá parkovací místa),
- Smart Enviroment (monitorování emisí, kontrola kvality ovzduší),
- Smart People (sdílení dat),

- Smart Living (inteligentní budovy).

Tabulka 1 specifikace jednotlivých sítí (16).

Technologie	Kmitočto-vé pásmo	Šířka kanálu	Přenosová rychlost	Maximální dosah	Standard
Sigfox	pod 1 GHz	100 Hz	100 b/s	3–50 km	proprietární
Weightless-N	pod 1 GHz	200 Hz	100 b/s	5–8 km	Weightless SIG
Nwave	pod 1 GHz	200 Hz	100 b/s	7–10 km	proprietární
WAVIoT NB-Fi	pod 1 GHz	100 Hz	10–100 b/s	10–50 km	proprietární
Telensa PLA-Net	pod 1 GHz	1250 Hz	60/500 b/s	2–8 km	proprietární
LoRaWAN	pod 1 GHz	125/250 kHz	0,25–50 kb/s	5–15 km	LoRa Alliance
RPMA	2,4 GHz	1 MHz	156/624 kb/s	5–8 km	proprietární
Weightless-P	pod 1 GHz	12,5 kHz	0,2–100 kb/s	2–5 km	Weightless SIG
DASH7	pod 1 GHz	25/200 kHz	9,6/55/166 kb/b	1–10 km	DASH7 Alli-ance
Weightless-W	400–800 MHz	5 MHz	0,001–1 Mb/s	5 km	Weightless SIG
HaLow	pod 1 GHz	1/2/4/8/16 MHz	0,15–18 Mb/s	2 km	IEEE 802.11ah
LTE-M	800/900 MHz	1,4 MHz	0,2–1 Mb/s	5–11 km	3GPP

Tabulka 2 ukazuje maximální efektivní vyzařovaný výkon (ERP) a omezení pracovního cyklu v těchto pásmech (LBT (Listen Before Talk), AFA (Adaptive Frequency Agility), převzato z (11).

Pásmo	**Max. výkon**	**Omezení pracovního cyklu**
863–870 MHz	≤ 25 mW e.r.p. (14 dBm)	≤ 0,1 % nebo LBT/AFA
868–868,6 MHz	≤ 25 mW e.r.p. (14 dBm)	≤ 1,0 % nebo LBT/AFA
868,7–869,2 MHz	≤ 25 mW e.r.p. (14 dBm)	≤ 0,1 % nebo LBT/AFA
869,4–869,65 MHz	≤ 500 mW e.r.p. (27 dBm)	≤ 10 % nebo LBT/AFA
869,7–870 MHz	≤ 25 mW e.r.p. (14 dBm)	≤ 1,0 % nebo LBT/AFA
869,7–870 MHz	≤ 5 mW e.r.p. (7 dBm)	bez omezení
870-875,8 MHz	≤ 25 mW e.r.p. (14 dBm)	≤ 1,0 % nebo LBT/AFA
915–921 MHz	≤ 25 mW e.r.p. (14 dBm)	≤ 0,1 % nebo LBT/AFA

V České republice jsou používány sítě LoRaWAN, Sigfox a NB-IoT. Nadále se v mé práci se budu zabývat pouze technologií Sigfox, hlavně kvůli jejímu velkému pokrytí a slibnému rozvoji v České republice. Navíc Sigfox oproti jeho konkurenci v ČR poskytuje mnohem lepší dosah v urbanizovaném prostředí. Hlavně díky této výhodě je Sigfox velmi slibným adeptem pro použití do vnitřních prostor, na místech, kde je implementace LoRaWAN nemyslitelná.

3 Sigfox

Sigfox operuje na technologii velmi úzkého pásma (UNB). Jeho hlavní výhodou je dosah, který při outdoorovém použití může být až 50 km, viz Tabulka 3. Ve městech mezi budovami se dosah pohybuje okolo 3-5 km. Výdrž modulu na baterii v síti Sigfox se pohybuje mezi 3 až 10 lety (17), také hodně záleží na frekvenci zasílání zpráv, při vysoké frekvenci může být výdrž baterie jen 3 roky.

3.1 Posílání dat

Při posílání dat v síti pošle modem pakety nesynchronizovaně všemi směry, každý paket pošle třikrát na třech různých frekvencích, proto lokální rušičky z principu nemohou fungovat. Pakety přijímá více BTS (základnová stanice), z nich se zprávy odesílají na cloud ve Francii. Z cloudu můžeme přebírat informace a zpracovávat je různými aplikacemi.

Přenos jedné zprávy trvá 3 až 6 sekund, obecně můžeme odeslat pouze 1 zprávu za 10 minut, což je 144 zpráv denně. Sigfox by zvládl odesílat i více zpráv, avšak je regulován ČTÚ, dle *všeobecného oprávnění č. VO-R/10/11.2016-13* (12). Spadá do tzv. s-třídy, která určuje, kolik procent času za jeden den může zařízení vysílat. U s-třídy v tomto spektru je to 1 %, což znamená 24*1 %=864 sekund, odeslání každé zprávy ze zařízení trvá 2 sekundy, 864/2=432 sekund. Sigfox posílá každou zprávu 3x, proto 432/3= 144 zpráv za den. Pro zpětnou komunikaci mezi modulem a anténou je zde povoleno pouze 8 bytový downlink (zpětný kanál), který můžeme provést pouze 4x denně (18).

3.2 Parametry

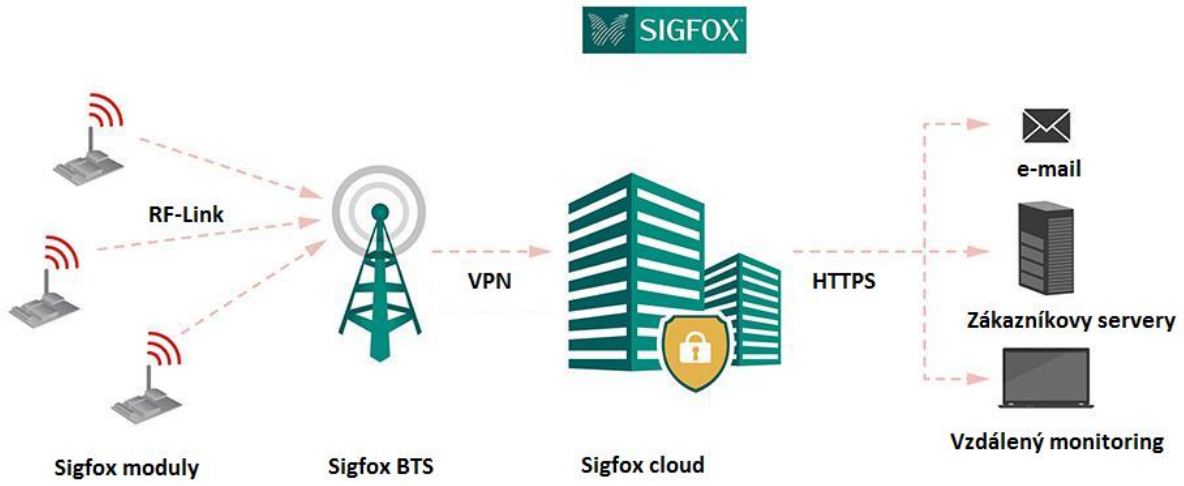
Výkon zařízení je 25 mW, který je vtěsnaný do velmi úzkého pásma a robustní DBPSK (17) modulace, což zaručuje takto velký dosah. Pro srovnání, podobný výkon má i ovladač od centrálního zamykání vozidla, ten ovšem operuje v širším pásmu, proto je jeho dosah o tolik menší (17).

Tabulka 3 parametry Sigfox převzato z (19) a (17).

Velikost zprávy	0–12 bytů
Frekvence	868MHz (EU), 915 MHz (USA)
Rychlost přenosu	100 b/s
Výkon	25mW / 14 dBm
Zpětný kanál	4 zprávy po 8 bajtů denně
Dosah v terénu	až 50 km v terénu, 3 km ve městě pro indoor
Výdrž na bateriích	3–10 let
Pokrytí	polovina Evropy, staví se USA, LATAM a další
Zařízení v síti	Cca 10 000 000
Pokrytí v ČR	92 % území
Maximální počet zařízení na 1 BTS	100 000

3.3 Architektura sítě

Síť Sigfox používá hvězdicovou topologii (Obrázek 1). Hlavní výhodou je to, že moduly jsou na sobě nezávislé, takže rušení jednoho zařízení neovlivní funkčnost ostatních. Další výhodou je snadné vyhledání problému v síti, neprobíhá kolize mezi pakety jednotlivých zařízení. Nevýhodou je, že při výpadku řídícího prvku vypadne celá část sítě, avšak tento problém je řešen používáním více BTS, na které zařízení současně vysílají.

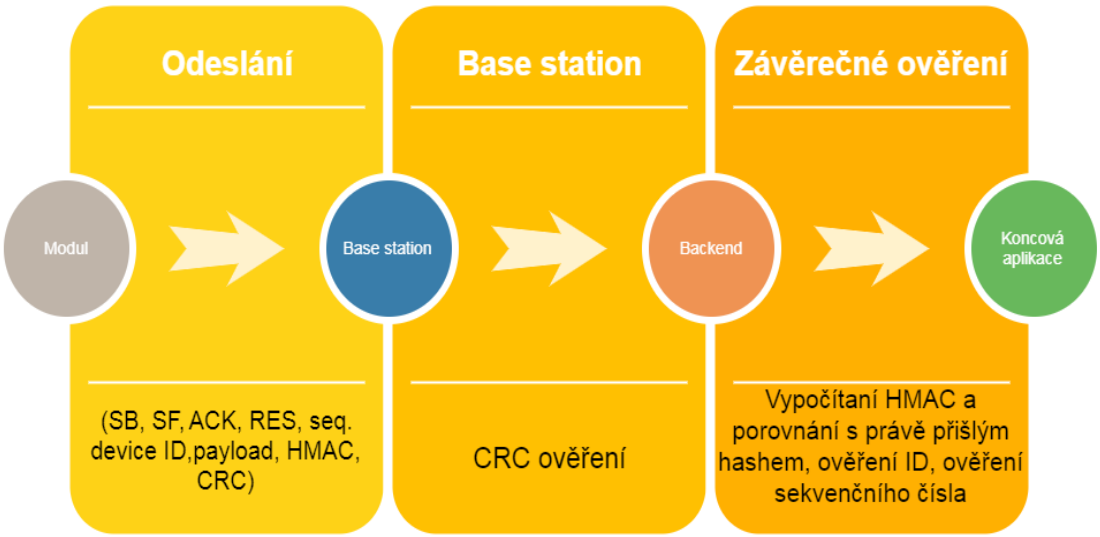


Obrázek 1 architektura sítě Sigfox převzato z (20).

3.4 Zabezpečení

Při odesílání zprávy máme 12 bytový payload (zpráva), kromě něj se posílá tzv. režie, která má 14 bytů. Režie obsahuje řadu bezpečnostních prvků:

- ID - Jedinečné číslo, které identifikuje zařízení,
- Sekvenční číslo (seq)- Uložené v EEPROM, čísluje zprávy, chrání proti nelegálním klonům, maximální hodnota 4096,
- CRC8 (21)- ověřuje zda zpráva nebyla pozměněna,
- SB- send bit message (0,1),
- SF- Sigfox frame (rámec),
- ACK- acknowledgment (potvrzení), 8byte zpráva nastavená v našem backendu,
- HMAC- Z ID zařízení se vygeneruje haš.



Obrázek 2 posílání zprávy v Sigfox, informace převzaty z (21).

Bohužel je zde absence, jakéhokoliv šifrování zpráv, od modulu až k Backendu (cloudu). BTS jsou připojené přes VPN ke cloudům. Z cloudu je zde aplikované standartní internetové šifrování SSL. Sigfox neustále rozšiřuje a vylepšuje svoji síť, např. plánuje implementaci šifry AES-128. Podrobnější architekturu sítě vidíme na obrázcích 1 a 2. Je vidět, že síť Sigfox je relativně dobře zabezpečena, až na jednu věc a to je zaručení důvěrnosti (prevence neautorizovaného vyzrazení dat) zpráv.

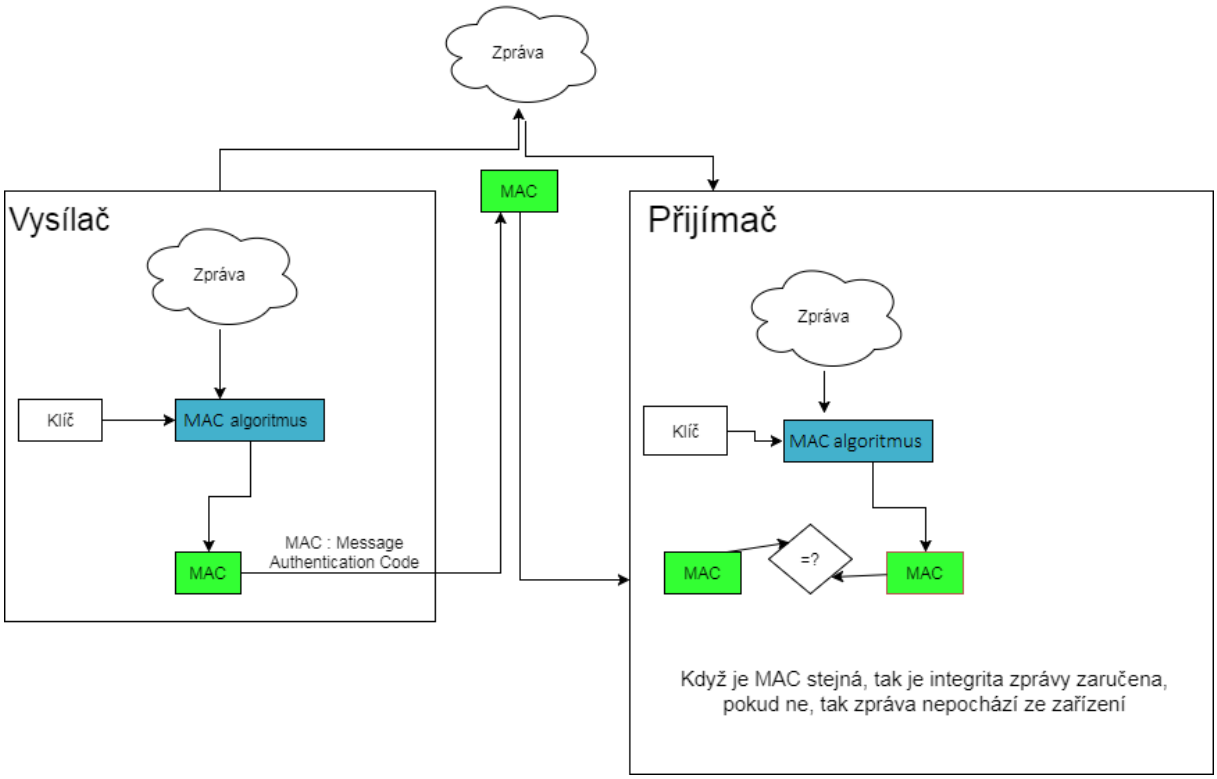
3.4.1 HMAC

Ověření MAC je pro síť Sigfox z bezpečnostního hlediska velmi důležité. Každé zařízení je během výroby opatřeno unikátním ověřovacím symetrickým klíčem, ze kterého se vypočítá unikátní nezaměnitelný token, viz Obrázek 3, ten se pak odesílá pokaždé v režii se zprávou. Token nám pak zajišťuje ověření (autenticitu) odesílatele a integritu zprávy samotné. Dále nám spolu se sekvenčním číslováním zaručuje nepopiratelnost zpráv (21).

3.4.1.1 Co nám HMAC tedy zaručuje:

- Integrita (21), také celistvost nám zaručuje, že zpráva nebyla nijak modifikována či pozměněna.
- Autenticita nám zajišťuje, že zpráva pochází opravdu z našeho zařízení a není vytvořena útočníkem.
- Nepopiratelnost, nám zaručí, že jsme opravdu autorem zpráv.

3.4.1.2 Jak funguje HMAC



Obrázek 3 schéma fungovaní MAC algoritmu převzato z (21).

Schéma obsahuje proces vytvoření a ověření MAC. Na straně vysílače je zpráva s unikátním klíčem vytvořeným při výrobě zařízení vložena do MAC algoritmu, ten vygeneruje jedinečný haš, který pošle po síti Sigfox. Na straně příjemce se provede obdobný proces a znovu vypočítaný haš se porovná s hašem, který došel přes síť Sigfox (21).

3.4.2 Cyklický redundantní součet

CRC8 se v Sigfox využívá při kontrole chyb u posílaných zpráv, jeho velikost zabere 1 byte z režie a pomáhá nám hlídat změny v samotné zprávě (integritu zprávy) během jejího přenosu. V Sigfox síti se CRC součet provádí v modulu, ze kterého odesílá data a ověřuje se v BTS, viz Obrázek 2, pokud se součet neshoduje, tak je zpráva prohlášena za pozměněnou. CRC má více módů jako jsou CRC 4, 8, 32, 64, 128, číslo určuje stupeň polynomu, např. součet typu CRC8 má nejvyšší koeficient x^8 (22).

Existují i generující se polynomy, při kterých na straně ověřovatele vzniká konstantní hodnota. V praxi se vydělí binární hodnota odesílaného payloadu P s daným polynomem p, při dělení vznikne vždy číslo o jeden bit menší než daný polynom, pokud je polynom p, např. 234, nikdy nemůže být hodnota zbytku po dělení větší než 234. Výsledná hodnota se připojí ke zprávě a zajišťuje nám integritu zprávy (23).

$$CRC = P \bmod p$$

3.5 Zhodnocení zabezpečení Sigfox

Sigfox je relativně dobře zabezpečen. Integritu, autentizaci a nepopiratelnost zpráv nám zaručuje HMAC a CRC, podrobně popsané výše. Jelikož zařízení v síti Sigfox nepoužívají ke komunikaci internetový protokol, autorizace jednotlivých modulů probíhá pomocí jedinečného sériového čísla. HMAC spolu se sekvenčním číslováním chrání před nelegálními klony v síti. Od BTS nám zaručují bezpečnost běžné internetové protokoly, k ochraně dat je zde využíváno VPN nebo HTTPS. Jediné, co síť zcela postrádá ochranu důvěrnosti dat. Zprávy nejsou šifrovány a to může být pro některé potencionální koncové uživatele jedna z věcí, která jim v Sigfox opravdu chybí, proto v následující kapitole navrhneme vhodné šifrování, které budeme moci implementovat do sítě Sigfox (21).

4 Návrh pro zvýšení bezpečnosti Sigfox

V kapitole, která se zabývala již implementovaným zabezpečením do sítě Sigfox jsme zjistili, že síť postrádá šifrování zpráv. Šifrování je pro tuto síť velmi důležité, z hlediska jejího využití. Sigfox má ambice se připojit do mnoha odvětví našeho života. Do zdravotnictví, kde Sigfox moduly mají plnit funkci monitorů zdravotního stavu či asistenčních technologií. Dále do veřejného sektoru, tam Sigfox může doplnit dosavadní komunikační sítě nebo může být implementován do systému zabezpečení, také nesmíme opomenout koncept chytrých měst a další zajímavé projekty, ve kterých má Sigfox velikou šanci na úspěch. Pro tyto všechny výše zmíněné projekty je nutná ochrana důvěrnosti zpráv. Tento problém si v kapitole 4 rozebereme a pokusíme se najít jeho vhodné řešení. Při výběru vhodného šifrování bude největší důraz kladen na energetickou náročnost šifry a bezpečnost dané šifry. Díky tomu, že Sigfox posílá zprávy dlouhé maximálně 12 bajtů, můžeme uvažovat i o implementaci šifry klasické jako je OTP.

4.1 Přehled dosavadních možností pro ochranu důvěrnosti zpráv

4.1.1 Asymetrické šifry:

K šifrování a dešifrování používáme odlišné klíče. Klíč k šifrování je veřejný a zpráva nejde klíčem zpětně dešifrovat. Pro dešifrování musíme použít klíč privátní. Hlavní výhodou asymetrických šifer je to, že pro šifrovanou komunikaci nemusíme distribuovat privátní klíč k odesílateli. Nevýhodou je velká výpočetní náročnost a délka veřejného klíče potřebného pro bezpečné zašifrování zprávy, proto jsou pro naše účely lepší šifry symetrické (24).

Příklady asymetrických šifer:

- RSA,
- ElGamal,
- Kryptografie nad eliptickými křivkami,
- Kryptografie s Lucasovými funkcemi.

4.1.2 Symetrické šifry:

Pro zašifrování i dešifrování zprávy se používá pouze jeden klíč. Výhodou symetrických šifer je nízká energetická náročnost. Nevýhodou je naopak složitá distribuce klíče, který nesmí být nijak zkompromitován. Symetrické šifry se dělí na dva základní druhy blokové a proudové (25).

4.1.2.1 Blokové šifry:

- AES,
- CAST,
- DES,
- IDEA,
- RC2,
- RC5,
- 3DES.

U těchto šifer zprávu rozdělíme na bloky, které nezávisle na sebe zašifrujeme. Délka zašifrované zprávy je stejná jako délka vstupu. Jsou bezpečnější než proudové pro zasílání periodicky opakujících se zpráv. Dnes se nejvíce využívá verze šifry AES, která se implementuje do většiny moderních zařízení. Dokonce se uvažuje o implementaci této šifry do Sigfoxu (17).

4.1.2.2 Proudové šifry:

- RC 4,
- Vermanova šifra (OTP) – jedná se o šifru klasickou.

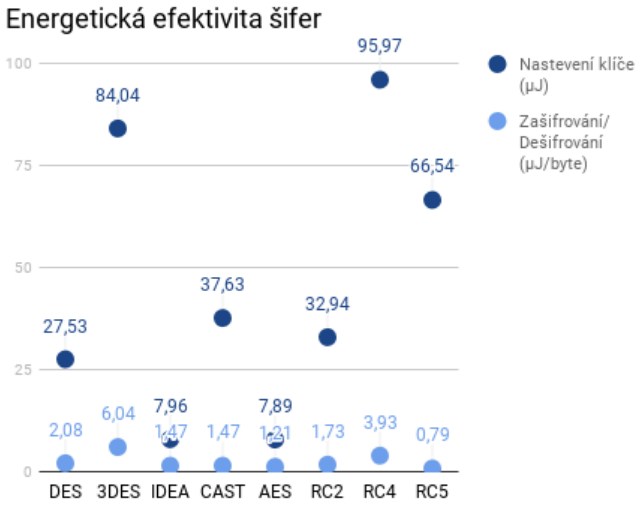
Jsou méně energeticky náročné než blokové šifry, ale jsou více náchylné ke kryptoanalytickým útokům. Zpráva se šifruje jako celek bitovým sčítáním s klíčem. Dělí se na synchronní a asynchronní šifry. U synchronních musíme zaručit přesnou synchronizaci se serverem nebo zašifrovanou zprávu již na serveru ne dešifrujeme. Velkou nevýhodou u těchto šifer je, že útočníkovi dovolujeme převracet bity ve zprávě (26). Narušení integrity nám ale u Sigfoxu hlídá CRC a HMAC, proto takové šifry můžeme bez obav použít.

4.2 Výběr vhodného šifrovacího algoritmu:

Šifry, které jsem neuvedl, nejsou vhodné pro šifrování 128 bitové zprávy nebo jsou zbytečně energeticky náročné. U výběru musíme vzít v potaz, že zprávy se mohou opakovat a pokud bychom měli stejný klíč, značně by se snížila bezpečnost šifry, proto navrhuji dát na začátek zprávy blok "náhodných" bitů nebo můžeme přidat inicializační vektor, který by nám měl zajistit vetší náhodnost i u periodických zpráv. Dále musíme zajistit čerstvost dat a integritu. Čerstvost dat můžeme zaručit sekvenčním číslováním, které dokáže Sigfox modul dělat automaticky. Kontrolu integrity nám zajišťuje HMAC a CRC součet již implementovaný do Sigfoxu, tyto věci byly již podrobně popsány v kapitole Sigfox. Naším algoritmem musíme zaručit důvěrnost zpráv, to znamená, že žádná osoba bez znalosti klíče nebude schopna obsah zprávy přečíst.

4.2.1 Hodnocení šifer dle různých hledisek:

- Energetická náročnost
- Bezpečnost



Obrázek 4 graf energetické efektivity šifer, převzato z (23).

Energetická náročnost je naším hlavním kritériem při výběru, nemůžeme si dovolit na našem zařízení provozovat příliš náročný šifrovací algoritmus, protože bychom značně ovlivnili výdrž baterie zařízení.

Ze získaných dat plyne, že AES je z šifer uvedených v grafu energeticky nejméně náročné. Nízkou energetickou náročností se také vyznačuje algoritmus OTP (27). V uvážení byl vzat i algoritmus IDEA, ale ten je velmi podobný algoritmu AES. Algoritmus DES byl dříve standardem v šifrování, avšak dnes je již velikost klíče příliš malá a dá se snadno prolomit útokem hrubou silou, algoritmus 3DES je 3x provedený DES, proto je jeho využití nevýhodné. Dnešním šifrovacím standardem je AES. Ostatní šifry jsou zbytečné pro šifrování, tak malé zprávy.

4.2.2 Hodnocení a podrobnější popis vybraných šifer:

4.2.2.1 AES (Advanced Encryption Standart):

AES, také Rijndael je velmi rychlá a nízko energetická bloková šifra (28). Byla schválena v roce 2001. Algoritmus využívá matici 4*4 byty, těleso $GF\ (2^8)$: $g\ (x) = (x^8 + x^4\ + x^3 + x^1 + 1)$. Naši 128 bit zprávu rozložíme na 4 bloky, každý blok má 32 bitů. Šifra může mít různě dlouhé klíče, delší klíč přidává algoritmu bezpečnost na úkor výpočetní náročnosti, velikost klíčů záleží na počtu rund (tabulka 4). Dnes se nejčastěji používají verze s 128 bitovým klíčem, které poskytují odpovídající ochranu a dobrou výpočetní a energetickou náročnost (28).

Algoritmus	Velikost klíče (bity)	Vstupní a výstupní blok	Počet rund
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Tabulka 4 velikost klíče převzato z (24).

Operace při šifrování:

- Záměna bytů: Každý byte zprávy je zaměněn za jiný dle tabulky.
- Prohození řádků: Řádky jsou v matici prohazovány. První řádek je prohozen o 0 míst. Druhý řádek je prohozen o 1 místo v tabulce.
- Kombinování sloupců: Zajišťuje náhodnost dat. Malá změna dat na vstupu kompletně změní data na výstupu.
- Přidání podklíče: Na počátku máme 128 bitový základní klíč, postupně na něm vytvoříme operací random dalších 10 pseudonáhodných rundovních klíčů. Každý rundový vygenerovaný klíč se operací XoR přičte k datům.

Bezpečnost AES závisí na délce klíče. V tabulce vidíme teoretický čas prolomení klíče v závislosti na jeho délce útokem brute force.

Velikost klíče	Čas do prolomení klíče
56 bitů	399 sekund
128 bitů	$1.02 \cdot 10^{18}$ let
192 bitů	$1.872 \cdot 10^{37}$ let
256 bitů	$3.31 \cdot 10^{56}$ let

Tabulka 5 čas prolomení AES (24).

Na našem zařízení by byla použita verze s 128 bitovým klíčem, opět kvůli energetické a výpočetní náročnosti, která je mnohonásobně větší u 192 bitových klíčů a 256 bitových klíčů. Délka klíče by měla být dostačující, proti brute force útokům, viz Tabulka 5. Šifra je velmi náchylná na útok postranními kanály (29).

AES módy, které uvažuji:

ECB mód by se neměl používat, pokud se šifruje více než jeden blok dat se stejným klíčem. U ECB se zpráva rozdělí do bloků, každý blok se šifruje samostatně, avšak ECB dnes poskytuje chabou ochranu periodickým zprávám, protože šifruje stejný blok textu na stejný blok šifrované zprávy, to znamená, že zašifrovaný text není náhodný.

CBC, OFB a CFB jsou podobné. Ve většině prací se CBC uvádí jako nejlepší (29), díky tomu, že se při šifrování využívají i předchozí bloky zprávy, a proto je zaručena její náhodnost. Pokud bychom zaručili integritu a autentizaci vykonávanou na straně serveru.

CTR použijeme místo CBC / OFB / CFB, pokud chceme mít dobrou paralelizaci (rychlost). Bohužel, funguje na principu převádění blokové šifry na proudovou a využívá multitasking. To znamená, že její energetické náročnost je vysoká.

OCB je zdaleka nejlepší režim, protože umožňuje šifrování a autentizaci v jediném průchodu. Použití šifry je ale chráněno patentem, proto ji nemůžeme použít.

XTS bychom měli používat, pokud šifrujete náhodně přístupná data (ram, harddisk) a nikoli stream.

Měli bychom používat jedinečný náhodný inicializační vektor (IV) při každém šifrování. Existují i další módy AES, ale ty se pro naše účely nehodí, kvůli pomalejšímu zpracovávání dat (30). CBC s 128 bit klíčem je jednou z použitelných variant, při teoretické životnosti zařízení 10 let bych do zařízení nahrál 10 klíčů, které by se každý rok automaticky vyměnili, tím pádem bychom značně navýšili bezpečnost našeho šifrování.

4.2.3 OTP

Vermanova šifra je jediná neprolomitelná šifra, protože obsahuje pouze informaci o délce zprávy. Je velmi úsporná. Dokáže rychle a efektivně zašifrovat 128 bitů payloadu. Problém nastane při zaručení integrity, útočník může náhodně měnit jednotlivé bity zprávy.

4.2.3.1 Podmínky funkčnosti šifry

- Klíč se nikdy nesmí opakovat, pokud by se opakoval, dala by se šifra snadno rozluštit.
- Klíč musí být dokonale náhodný, nelze použít generátory pseudonáhodných čísel, proto musíme nalézt vhodný generátor opravdu náhodných čísel, nejlépe použít hardwarový generátor nebo speciální programy, které čísla generují z proměnných jako je teplota, čas, počet spuštěných oken, souřadnice myši.

- Klíč musí být stejně dlouhý jako přenášená zpráva.

4.2.3.2 Možnosti útoku

Při splnění všech podmínek pro funkčnost šifry je statická kryptoanalýza znemožněna kvůli náhodnému klíči, který je xorován ke zprávě, proto i výsledný zašifrovaný text je 100% náhodný, proto z něj nelze zjistit žádné informace o spojitosti mezi znaky nebo jejich počtu (31).

Ani útok hrubou silou (32), vůči kterému není odolná prakticky žádná jiná šifra, neuspěje. I kdyby měl útočník k dispozici neomezený výpočetní výkon, kvantové počítače a podobně a mohl systematicky vyzkoušet všechny možné klíče délky *n*, pak výsledkem snažení bude pouze posloupnost všech možných zpráv délky *n*. Útočník mezi nimi nebude schopen nalézt tu správnou, nezíská o ní žádnou informaci. Ani z četnosti znaků ve zprávách, které útočník získal, nedokáže nic zjistit, ale to pouze za předpokladu, že klíče jsou zcela náhodné. (33)

4.2.3.3 Nepodmíněná bezpečnost

Znamená, že bezpečnost šifry není závislá na technických možnostech protivníka, takovou míru bezpečnosti dnes nabízí kvantová kryptografie a Vermanova šifra (31).

4.2.3.4 Bezpečnost a využití

Dnes se Vermanova šifra využívá jen zřídka, z důvodu složitého generování klíčů, avšak toto platí například pro 50 GB dat, kde musí být klíč stejné velký jako data sama. My ale generujeme klíče pro šifrování 525600 dvanácti bytových zpráv, což nebude tak obtížné, vzhledem k životnosti našeho zařízení a omezení odeslaných zpráv za den není potřeba databáze klíčů tak obsáhlá. Pokud tedy zaručíme, že námi vygenerované klíče budou náhodné a při přenosu nebudou zkompromitovány, bude naše šifrování velmi složité rozluštit. C. E. Shannon v roce 1949 matematicky dokázal nerozluštitelnost Vermanovy šifry, ale musí být dodrženy podmínky zmíněné výše (34). V praxi je Vermanova šifra implementována například do internetového bankovnictví v Jižní Koreji, kde pomáhá chránit hesla klientů (35).

4.3 Shrnutí výběru

Samotné hodnocení z předešlé podkapitoly jsem sumarizoval do tabulky číslo 6, kde můžeme vidět, že pro naše účely je vhodnější OTP. Nároky na paměť jsou stejné z důvodu toho, že u CBC budeme potřebovat místo pro náhodné inicializační vektory a u OTP pro samotné klíče Hodnocena byla bezpečnost při šifrování zprávy při používání 128 bitových klíčů, také energetické nároky, nároky na paměť. Rychlost provedení operace šifrování je srovnatelná. AES 128 bit klíčem je neprolomitelná útokem hrubou silou další $1{,}02 \cdot 10^{18}$ let, při dnešním výpočetním výkonu. Pokud bychom zahrnuli do výpočtu vývoj technologií, udává se, že 128 bit klíč bude bezpečný

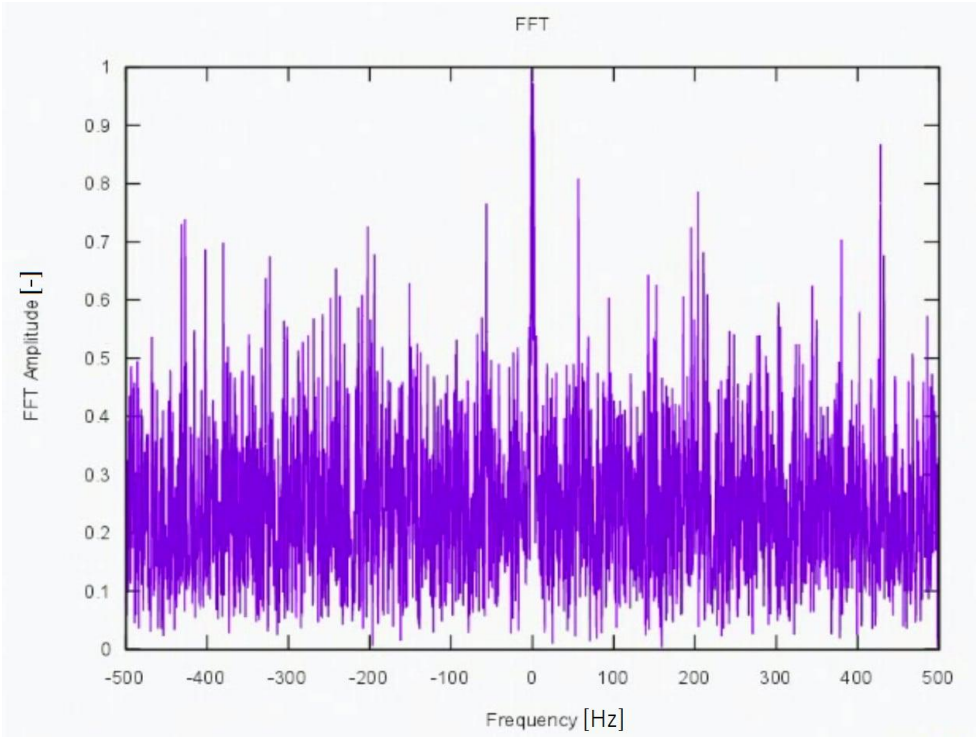
dalších 30 let (24). U OTP výpočetní výkon nemá vliv na dobu prolomení šifry. Šifra se považuje za neprolomitelnou. Energetické nároky jsem určoval dle složitosti algoritmu a nutnosti připojení externích zařízení. U AES je značná složitost výpočetních operací při šifrování a u námi vybraného módu je nutné připojit externí úložiště pro IV, proto se domnívám, že OTP je méně energeticky náročné, protože šifrovací operací je XoR a je u něj také nutné připojit externí úložiště. Z výše uvedených důvodů jsem se rozhodl implementovat na naše zařízení v síti Sigfox šifru OTP.

Šifry	Bezpečnost	Energetické nároky	Nárok na paměť	Rychlost provedení šifrování
AES 128 CBC	neprolomitelné dalších 30 let	střední	střední	srovnatelná
OTP	neprolomitelné	Nízké	střední	srovnatelná

Tabulka 6 zhodnocení šifer.

4.4 Návrh vybraného šifrování

Vybrali jsme šifru OTP. O její bezpečnosti jsme se ujistili v kapitole 4. Klíče budou ukládány v podobě textového souboru na externí SD kartu, v souboru budou klíče uloženy po 12 bajtech v 1D poli. SD kartu zapojíme do Arduina pomocí čtečky SD karet popsané v kapitole Hardware. Samotné generování klíčů bude probíhat na hardwarovém generátoru, který dokáže generovat opravdu náhodné klíče. Pro naše potřeby jsem zvolil generátor Chaoskey, který se připojí do USB počítače a dokáže generovat 1 MB náhodných čísel za sekundu. Na grafu Fourierovi transformace můžeme vidět, že se neprojeví žádná dominantní frekvence, tím je dokázáno, že zařízení opravdu generuje náhodná čísla (36). Klíče tedy budou splňovat podmínky nutné k funkčnosti šifry popsané v kapitole 4.2.3.. Pokud budeme odesílat 144 zpráv denně po dobu 10 let, budeme muset ukládat na SD kartu 6,302 MB klíčů, což není mnoho. Proces šifrování je popsán v následující kapitole.

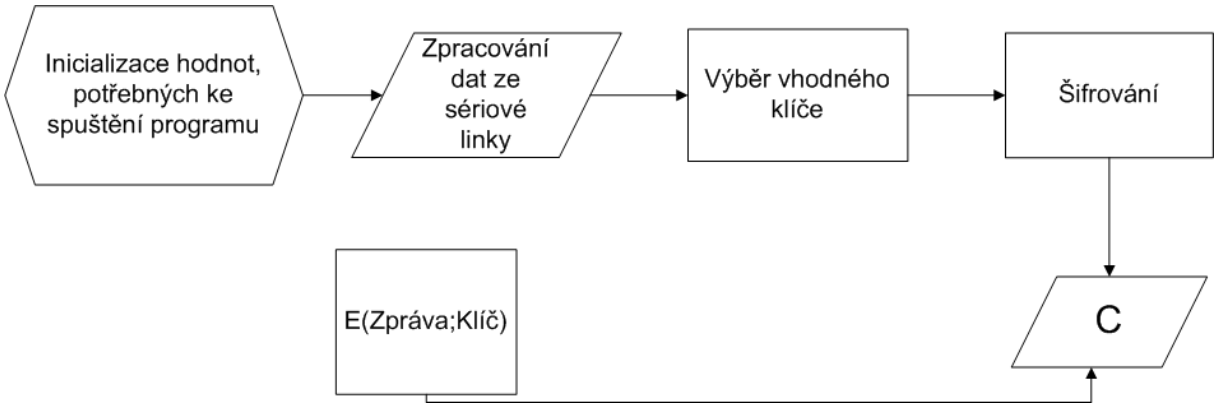


Obrázek 5 graf Fourierovi transformace (36).

5 Implementace šifry

5.1 Princip fungování algoritmu

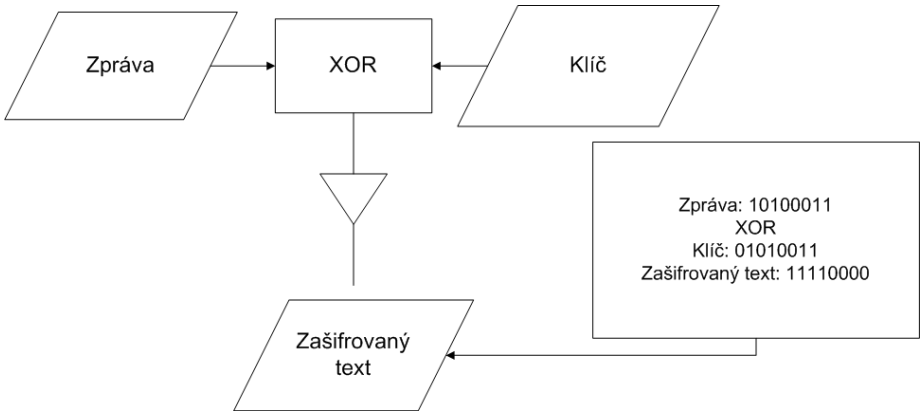
Na Obrázek 6, můžeme vidět popis fungování našeho algoritmu, již z tohoto diagramu je zjevné, že je algoritmus velmi jednoduchý a výpočetně málo náročný. Inicializace hodnot obnáší kontrolu toho, zda jsou SD karta a LPWAN modul správně zapojeny, dále se zde spouští softwarová i běžná sériová linka. Program naslouchá na sériové lince a čeká na input, po zadání inputu, se z SD karty vybere klíč, dle sekvenčního čísla zprávy a provede se samotný proces šifrování, který bude více popsán v kapitole Šifrování. Výsledkem tohoto procesu je zašifrovaný text, který se z modulu odešle pomocí softwarové linky do sítě Sigfox.



Obrázek 6 blokové schéma popisující šifrovacího algoritmu.

5.2 Šifrování

Samotné šifrování je velmi málo náročné na výkon našeho zařízení, probíhá pomocí XORu (⊕) zprávy vložené ze sériové linky a klíče načteného z SD karty.



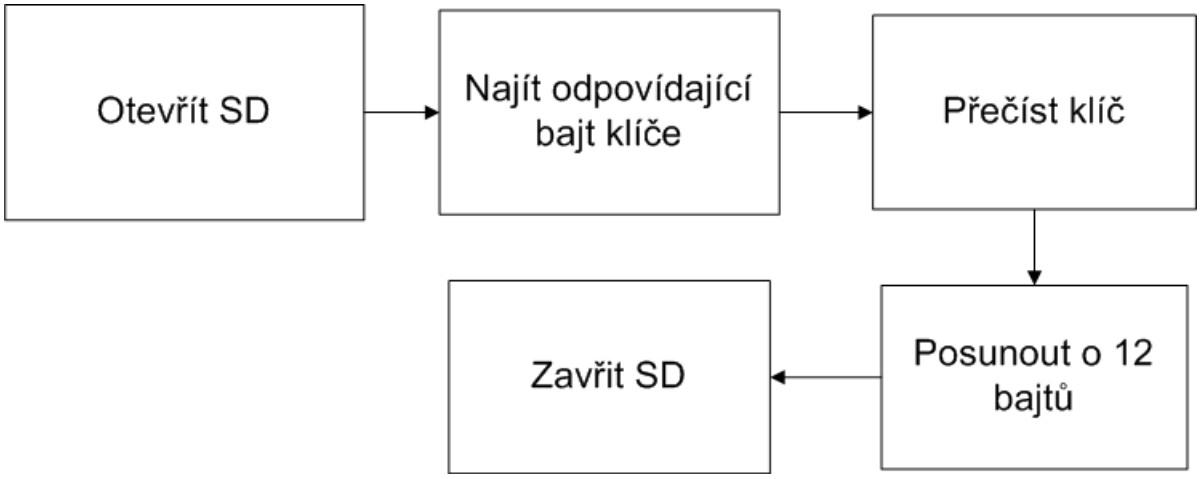
Obrázek 7 blokové schéma pro navrhnutou operaci XOR.

5.3 Databáze klíčů

Naše databáze klíčů je vytvořena v textovém souboru uloženém na SD kartě. Klíče jsou uložené po 12 bytových řádcích, každý řádek reprezentuje sekvenční číslo zprávy, pokud přeteče jeho maximální hodnota 4096, tak číslování započne znovu od nuly, viz kapitola Zabezpečení. Pro komunikaci s SD kartou zajišťuje základní knihovna pro Arduino (SD.h).

Jak již bylo uvedeno v kapitole Sigfox, výdrž zařízení na baterii je asi 3-10 let, pokud bychom tedy chtěli zařízení používat 10 let a chtěli bychom odeslat maximální počet povolených zpráv, potřebovali bychom 144*365*10= 525600 128 bitových klíčů, tedy potřebujeme 6,3072 MB paměti pro uložení všech klíčů. Na straně serveru budou nahrány stejné klíče, které se budou dešifrovat ve stejném pořadí, díky sekvenčnímu číslovaní zprávy. Pro generování náhodných klíčů je vhodné využít hardwarový generátor Chaoskey.

Reálně výběr klíče probíhá takto:



Obrázek 8 blokové schéma popisující průběh výběru klíče z SD karty.

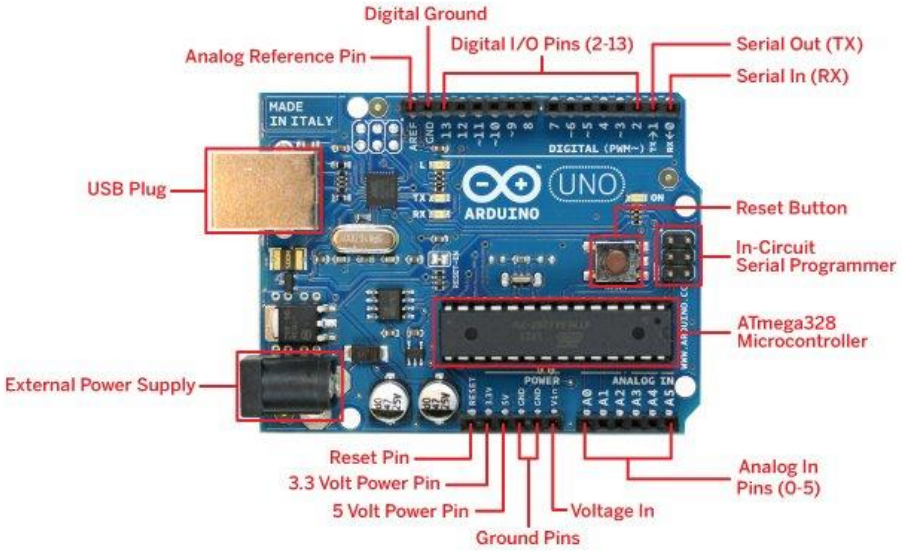
5.4 Hardware

Pro odesílání dat používáme Arduino UNO s připojeným modulem pro SD kartu a LPWAN modulem. Podrobnější popis daného hardwaru nalezneme v následujících podkapitolách.

5.4.1 Arduino Uno R3

Je nejpoužívanějším modelem mezi začátečníky i pokročilými. Má 6 analogových pinů a 14 digitálních, každý digitální pin můžeme použít jako 5 V napájení nebo zem, podle toho, jak jej programově definujeme, mimo to, máme možnost využít 3,3 V napájení. Arduino bude naší řídící jednotkou při šifrování a odesílání. Jeho úkol je načíst klíč z SD karty a provést XOR se zadanou

zprávou, poté zprávu odešle do našeho LPWAN modulu a z něj po softwarové sériové lince do sítě Sigfox. Při popisu vynechám námi nepoužívané piny, které jsou podrobněji popsány v této práci (37) . Dále máme možnost využít softwarovou sériovou linku na pinech 0 a 1, viz obrázek 9.



Obrázek 9 Arduino schéma pinnoutů, převzato z (38).

5.4.2 Procesor ATmega 328

Je to nízkoenergetický 8bit procesor, jeho rychlost se odvíjí od poskytnutého napětí procesoru, maximální možné napětí, jakému ho můžeme vystavit. Při 5,5 V je frekvence procesoru 20 Mhz (39), ovšem běžně se frekvence pohybuje kolem 16 Mhz, což je více než dostačující pro náš šifrovací proces. Čip obsahuje 16bitový časovač, který nám umožňuje provádět multitasking mezi jednotlivými procesy.

5.4.3 LPWAN modul

Tento modul budeme používat na odesílání zpráv do sítě Sigfox, pomocí AT příkazů, operační frekvence zařízení pro uplink je 868.130 MHz, pro downlink 869.525 MHz, během posílaní zprávy je běžná spotřeba 65 mA a při přijímaní 15 mA (40), v době nečinnost 2 µA. Zařízení je možno používat při teplotách od –30 °C do +85 °C (40). Minimální napětí, které zařízení smíme poskytnout je 1,8 V a maximální 3,3 V, proto můžeme zařízení rovnou připojit do Arduina bez potřeby redukce. Zařízení je drobné, jeho rozměry jsou cca 2,5 cm na výšku a 1,5 cm na šířku. K modulu také používáme anténu pro lepší konektivitu k síti. Pro připojení k Arduinu používáme pouze 4 piny (VCC 3,3 V; GND; TX; RX), viz Obrázek 12.

Obrázek 10 LPWAN node modulu sloužící ke komunikaci se Sigfox (41).

5.4.4 Anténa 868 Mhz

K LPWAN modulu připojíme anténu pro zesílení dosahu.

Specifikace (42):

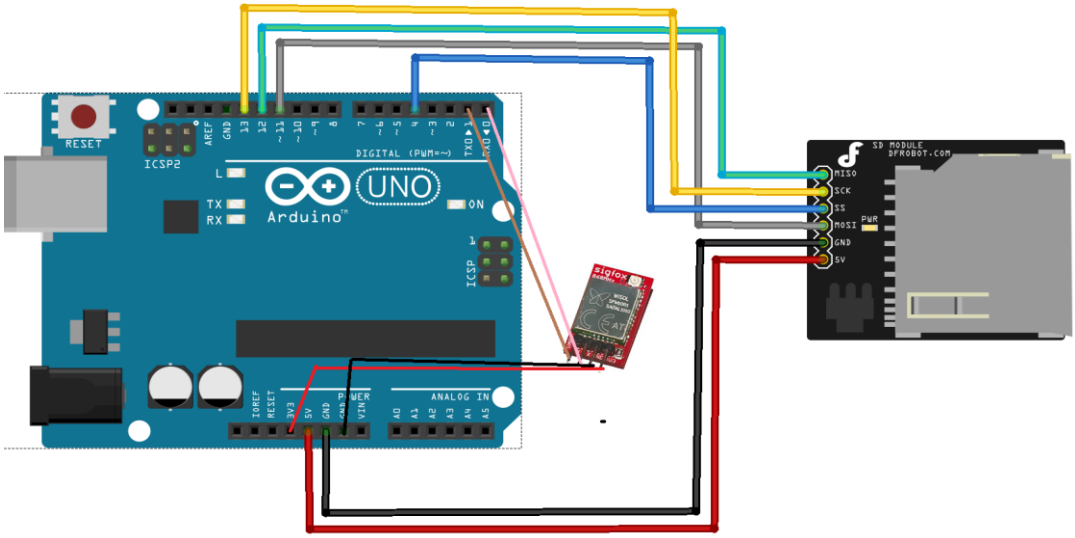
- Typ antény: všesměrová,
- frekvence: 868 MHz,
- zisk: 5dBi,
- impedance: 50 Ohm,
- VSWR: < 2,
- konektor: RP SMA (samice),
- pracovní teplota: -40 °C až 85 °C.

5.4.5 SD modul

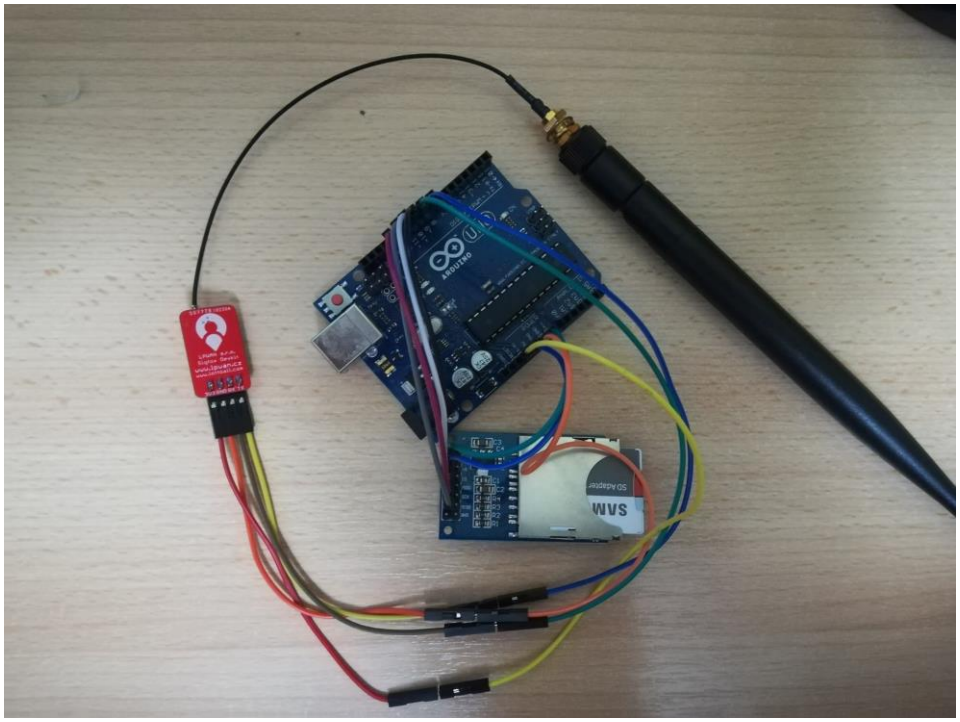
Pro rozšíření malé paměti zařízení, jsme využili přídavný SD modul, který použijeme pro ukládání klíčů. Na náš modul můžeme připojit až 2 Arduina, je ho možno napájet jak 3,3 V, tak i 5,5 V. Samotný modul dokáže nejen číst, ale i zapisovat do paměti SD karty. Pro jeho správnou softwarovou implementaci používáme základní knihovnu SD.h.

Obrázek 11 přídavný SD modul (43)

5.4.6 Schéma zapojení zařízení



Obrázek 12 schéma zapojení LPWAN NODE a SD modulu k Arduinu komponenty převzaty (44).



Obrázek 13 reálné zapojení komponent k Arduinu.

Červený drát u SD čtečky (Obrázek 12) vede do napájení 5 V, černý do země, ostatní dráty vedou na digitální piny. U LPWAN modulu růžový a hnědý drát vedou na piny RX a TX, těmito piny bude Arduino komunikovat s modulem, červený a černý drát jsou stejně jako u SD čtečky napájení s jedinou malou změnou je to, že napětí je místo 5 V jen 3,3 V.

5.5 Hrozby

Šifra je tedy bezpečná proti útokům směřujícím přímo na zprávu. Možnou hrozbou je pokus o zjištění klíčů fyzickým útokem na zařízení, např. vytažením a načtením SD karty nebo útok postranními kanály. Další z možností zjištění klíčů je útok na databázi umístěnou na serveru, pokud by útočník získal přístup k datům s klíči, mohl by nezjistitelně dešifrovat naše zprávy.

5.5.1 Řešení hrozeb

Proti fyzickým útokům popsaným výše, navrhuji aplikovat fyzickou obranu, krabičku zatavíme do pevného obalu, při jehož otevření modul pošle SOS zprávu, tím nás informuje, že byl obal porušen.

Před útokem postranními kanály nás chrání skutečnost, že každý klíč je jiný, čehož v praxi docílíme našim hardwarovým generátorem. V případě, že by útočník aplikoval na naše zařízení rušičku, zachytil zprávu, rozšifroval, upravil a znovu ji odeslal, bude neúspěšný, protože by neseděl CRC součet ani HMAC.

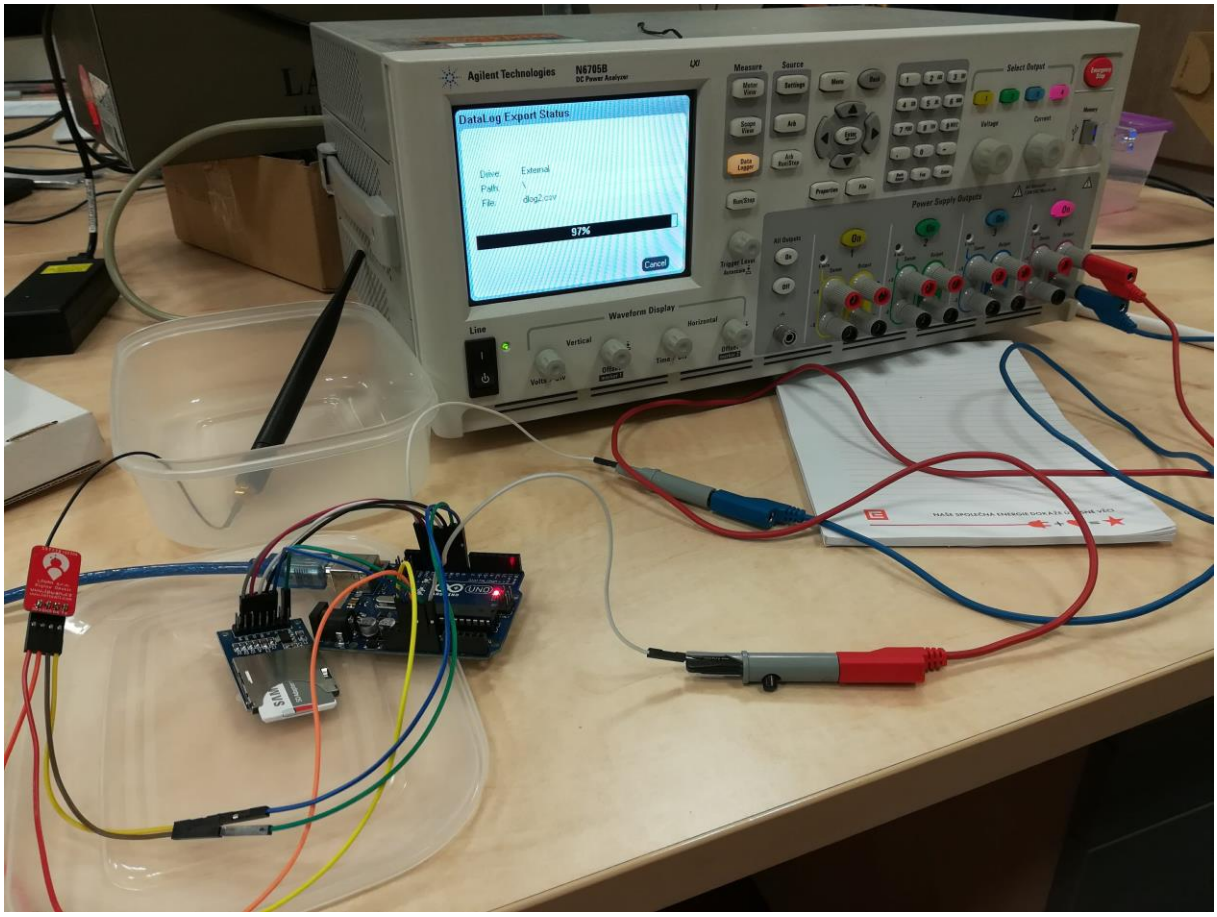
Pro ochranu klíčů uložených na serveru využijeme, tzv. Key wrap (dlouhodobé zašifrování klíčů pomocí 1 klíče). Při šifrování klíčů můžeme použít AES Key Wrap, který jim poskytuje vhodnou a je založen na AES (45). Stejným způsobem by bylo možné zajistit šifrování klíčů i na straně modulu, avšak tento proces by navýšil energetický odběr, proto se klaním raději k variantě s implementací fyzického zabezpečení.

6 Měření

V této kapitole budeme měřit efektivitu našeho algoritmu z mnoha hledisek:

- O kolik sekund průměrně zpomalí algoritmus proces odesílání,
- jaká je spotřeba energie při nečinnosti,
- jaká je spotřeba při odesílání zpráv bez algoritmu,
- jaká je spotřeba energie při odesílání zpráv s algoritmem.

Hodnoty byly měřeny pomocí analyzátoru odběru N6705B, viz Obrázek 14 zařízení pro analýzu odběru N6705B. Měřič jsme připojili pomocí pinů GND a Vin s Arduinem.



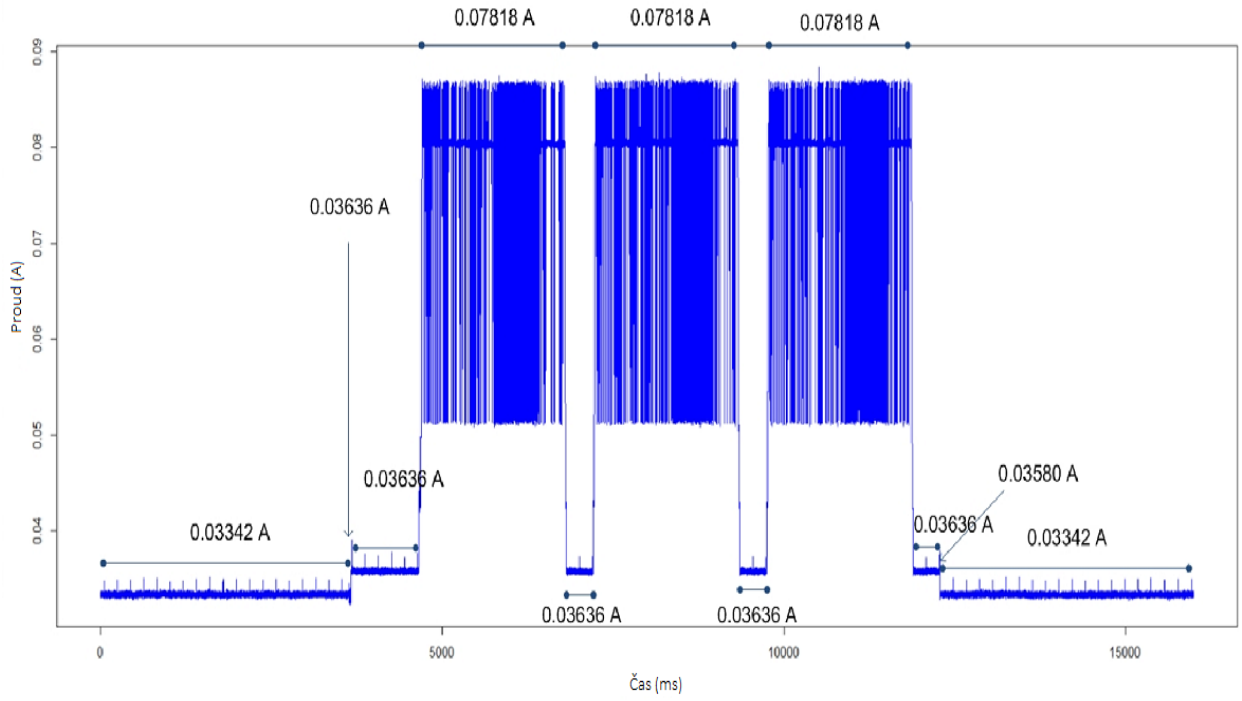
Obrázek 14 zařízení pro analýzu odběru N6705B.

6.1 Vliv šifrovacího algoritmu na dobu potřebnou pro odeslání zprávy

Do našeho algoritmu byl implementován příkaz millis(), díky kterému jsme mohli přesně měřit čas, za jaký se zpráva dostane do LPWAN modulu. Měření probíhalo nejprve na programu bez šifrovacího algoritmu a bylo opakováno 30x. Následně bylo provedeno měření s programem, kde šifrovací algoritmus implementovaný byl. Zjištěný průměrný čas šifrování je 253 ms.

6.2 Spotřeba při odesílání nezašifrovaných dat

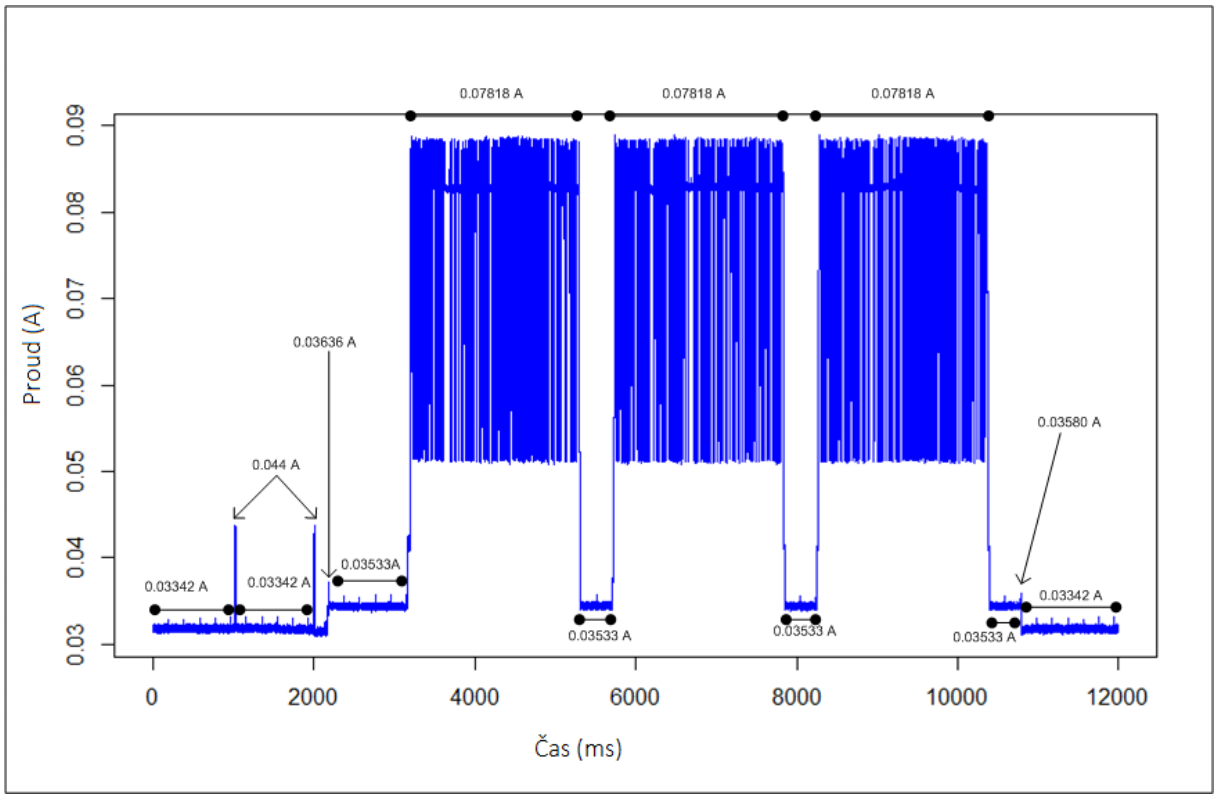
Měření probíhalo 2,5 minuty a bylo při něm odesláno 30 zpráv s 15 sekundovou prodlevou mezi jednotlivými zprávami. Interval snímání odběru byl 0,08 milisekund. Do grafu na Obrázek 15 jsem zahrnul hodnoty vytvořené jedním odesláním zprávy. Odběr zařízení není nijak razantní. Na grafu je vidět, že spotřeba vzroste nad 0,036 A pouze při posílání a zpracovávání zprávy. Malá špička o hodnotě 0,036 A je zpracovávání režie. Při odesílání se odběr pohybuje kolem průměrné hodnoty 0,078 A. Odběr je značně navýšen komponenty, které jsou součásti desky Arduino, ale nejsou nezbytné pro běh našeho algoritmu. Pokud bychom tyto komponenty odstranili, výrazně bychom tím snížili spotřebu energie, avšak prioritním cílem nebylo zredukovat spotřebu Arduina, ale vytvořit efektivní šifru, to se nám podařilo.



Obrázek 15 graf odběru v zařízení bez implementovaného šifrovacího algoritmu.

6.3 Spotřeba při odesílaní dat s šifrovacím algoritmem

Toto měření probíhalo 2,5 minuty, bylo při něm odesláno 30 zpráv s prodlevou 15 sekund mezi nimi. Interval snímání odběru byl nastaven na 0,02 milisekund. Celý proces před odesláním zprávy (i s šifrováním) trvá, dle grafu (Obrázek 16) cca 1000 ms, jeho průměrný odběr činní 0,0347 A. V porovnání s odesláním zprávy jde o minimální navýšení. Můžeme vidět 3 špičky, první z nich je způsobena použitím SD modulu pro načtení klíče (0,044 A), druhá je vytvořena šifrováním zprávy samotné (0,044 A), poslední je odběr při vytváření režie zprávy (0,03636 A). Tyto 3 špičky jsou zanedbatelné, pokud je přirovnáme k odběru LPWAN modulu (0,07818 A). Z grafu je tedy zřejmé, že naše šifra je energeticky velmi úsporná a je možno ji používat i na zařízeních umístěných v odlehlých oblastech, kde je výdrž baterie klíčovou vlastností.



Obrázek 16 graf odběru zařízení s implementovaným šifrováním.

6.4 Zhodnocení měření

Bylo zjištěno, že námi sestavený modul při nečinnosti má odběr kolem 33 mA. Pro snížení odběru lze použít také knihovnu pro sleepmode(mód spánku), např. Low-Power master, Sleep_N0m1 atd.. V tabulce na Obrázek 17 spotřeba Arduina při použití knihovni Low-Power master (47)., jsou zapsány hodnoty pro knihovnu Low-Power master. Výsledky měření jsou uspokojivé a dokazují, že se nám podařilo vytvořit nízko energetické šifrování. Šifrování nijak výrazně nezpomaluje chod kódu, jelikož samotný proces odeslání zprávy do sítě Sigfox zabere cca 6 sekund a šifrování samotné se provede v čase kolem 250 ms. Naším hlavním cílem nebylo snížit spotřebu zařízení knihovnami pro sleepmode, ale měli jsme vytvořit šifrovaní, které znatelně nenavýší odběr zařízení.

Vcc **(V)**	Rychlost jádra **(MHz)**	Spotřeba při aktivitě **(mA)**	Sleep mode **(uA)**
5.0	16	13.92	6.2
5.0	8	9.03	6.2
3.3	16	6.48	4.3
3.3	8	3.87	4.3

Obrázek 17 spotřeba Arduina při použití knihovni Low-Power master (47).

Závěr

Cílem této práce bylo navrhnout a implementovat kryptosystém, který by vyřešil dosavadní absenci mechanismu pro zaručení důvěrnosti zpráv v síti Sigfox. Proto jsme provedli důkladnou analýzu možných kryptosystémů, které by dokázaly co nejlépe využít již existující bezpečnostní prvky sítě. Výběrem šifry OTP jsme zajistili rychlé, bezpečné a hlavně nízkoenergetické E2E šifrování pro uživatele Sigfox, které může být nadále rozšířeno a uvedeno do praxe. Šifrování zajistí ochranu dat posílaných v síti, je připraveno k okamžité implementaci do současných aplikací po celém světě (čidla operujících v chytrých městech, GPS trackery, lékařské technologie, atd.). Vše je založeno na hloubkové analýze a posouzení nejvhodnějšího řešení. Účinnost našeho šifrování můžeme podložit měřeními, které potvrdily funkčnost a účinnost šifry. Hodnoty odběru při provádění operace šifrování se pohybují kolem 0,04 A a ve srovnání s průměrnými hodnotami při odesílání zprávy jsou více než zanedbatelné. Závěrem bych chtěl uvést, že se nám efektivně podařilo vyřešit jeden z velkých problémů této sítě, o kterém se vedlo mnoho debat na diskuzních fórech.

Literatura

1. **Simplecell.** Simplecell Connecting things. *Simplecell.* [Online] [Citace: 10. Únor 2018.] https://simplecell.eu/.

2. **Sigfox.** Simplecell Spot'it. *Simplecell.* [Online] https://simplecell.eu/sigfox-predstavuje-spotit-prvni-globalni-lokalizacni-sluzbu-bez-nutnosti-pouziti-gps/.

3. —. Sigfox boyard. *Sigfox partners.* [Online] [Citace: 12. Leden 2018.] https://partners.sigfox.com/companies/bayard.

4. **Sedlák, Jan.** Internet věcí. *Lupa.* [Online] 2017. https://www.lupa.cz/clanky/sigfox-internet-veci-bez-internetu-a-jen-pro-nektere-veci/.

5. **Columbus, Louis.** Forbes IOT market. *Forbes.* [Online] https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#3bdcaf19609b.

6. **Ammar, Rayes a Samer, Salam.** *Internet of Things From Hype to Reality: The Road to Digitization.* 2017.

7. **Sigfox.** *Secure Sigfox ready devices.* 2018.

8. **Ivan, Eroshkin.** *Řízení technologických procesů v koncepci IoT.* 2017.

9. **Leung, Omar Elloumi JaeSeung Song Yacine Ghamri-Doudane Victor C.M.** *Internet of Things (IOT) /M2M.*

10. **Lopez research.** *An Introduction to the Internet of Things.* místo neznámé : Lopez research, 2013.

11. **Hrstka, Jaroslav.** http://www.netguru.cz/novinky/3707-sitove-technologie-lpwan-pro-internet-veci-1-dil. *Netguru.* [Online]

12. **Český telekomunikační úřad.** *Všeobecné oprávnění č. VO-R/10/11.2016-13.* 2016.

13. **Hauser, Vojtěch.** *Bezpečnost v stítích LPWAN/LPN pro.* Praha : autor neznámý, 2016.

14. **Claire Goursaud, Jean-Marie Gorce.** *Dedicated networks for IoT : PHY.*

15. **Noronha, a další, a další.** *Internet of Everything (IoE) Value Index.*

16. **Vojtěch, Hauser.** http://www.netguru.cz/novinky/3792-sitove-technologie-lpwan-pro-internet-veci-4-dil. *NetGuru.* [Online]

17. **Tomáš, Poláček a Kolář, Filip.** Sigfox pro IoT. *Bastlířské středy.* 2017.

18. **Jan, Hofman.** Systém pro sběr technologických dat v koncepci IoT. [Online]

19. Technologie Sigfox. *Simplecell.* [Online] 2017. https://simplecell.eu/technologie-sigfox/.

20. Sigfox. *Cooking hacks.* [Online] 2017. https://www.cooking-hacks.com/documentation/tutorials/sigfox-connectivity-arduino-raspberry-pi-868mhz-europe-900mhz-us/.

21. **Sigfox.** *Technical Overview.* 2017.

22. **součet, Cyklický redundantní.** Algebra v informatice. *Vyučované předměty.* [Online] 8. Srpen 2008. http://class.pedf.cuni.cz/Jancarik/DesktopDefault.aspx?tabindex=0&tabid=21&PrvekID=262&portalsekce=2&KategorieID=98&Nezobrazovat=ano.

23. **Sobolewski, John S.** *Encyclopedia of Computer Science.*

24. **Fujdiak, Radek.** *ANALÝZA A OPTIMALIZACE DATOVÉ KOMUNIKACE PROTELEMETRICKÉ SYSTÉMY V ENERGETICE.* 2017.

25. **Hans Delfs, Helmut Kneb.** *Introduction to Cryptography: Principles and Applications.*

26. **Mareš, Martin.** Praktická kryptografie (Martin Mareš, Smršť 2015).

27. **Croft a Olivier.** *Using an approximated One-Time Pad to Secure Short Messaging Service (SMS).* místo neznámé : Information and Computer Security Architectures (ICSA) Research Group.

28. **Kumar, Jawahar a Thakur, Nagesh.** *DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis.*

29. **Ondřej, Semrád.** *Útok rozdílovou odběrovou analýzou na implementaci algoritmu AES na platformě Xilinx.*

30. **Švenda, Petr.** *Basic comparison of modes for authenticated-encryption (iapm, xcbc, ocb, ccm, eax, cwc, gcm, pcfb, cs).* 2016.

31. **Hála, Vojtěch.** Kvantová kryptografie. *Aldebaran bulletin.* 2005, Sv. III, 14.

32. **Bernstein, Daniel J.** *Understanding brute force.*

33. **Singh, Simon.** *Kniha kódů a šifer.*

34. **Fu-Guo, Deng a Gui Lu, Long.** *One-time Pad.* 2004.

35. **Yoo, a další, a další.** *Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. Multimedia Tools and Applications. 74. . 10.1007/s11042-014-1888-3.* 2014.

36. Root: Bastlírna. *Root.cz.* [Online] 11. listopad 2016. https://www.root.cz/clanky/chaoskey-skutecny-generator-nahodnych-cisel-do-usb/.

37. **AIAA OC Rocketry .** *ARDUINO UNO Revision 3 BOARD.* 2017.

38. Arduino Uno R3. *Robotics Nepal.* [Online] http://roboticsnepal.com/arduino-uno-r3.html.

39. **ATMEL.** *ATMEL 8-BIT MICROCONTROLLER WITH 4/8/16/32KBYTES.* 2009.

40. **LPWAN.** *LPWAN SigFox node.* místo neznámé : LPWAN, 2017.

41. LPWAN Sigfox node. *Arduino shop.* [Online] 2017. https://arduino-shop.cz/iot-bezdratove-periferie/1763-iot-lpwan-sigfox-node-1503052531.html.

42. LPWAN anténa 868 Mhz. *Arduino-shop.cz.* [Online] 2017. https://arduino-shop.cz/arduino/2009-antena-868mhz-5dbi-propojovaci-kabel-k-antene-rp-sma-samice-ipx-1.13.html.

43. **Geetech.** Arduino SD module. *Geetech.* [Online] https://www.geeetech.com/wiki/index.php/Arduino_SD_card_Module.

44. Arduino SD card example. *Get micros.* [Online] 2008. http://www.getmicros.net/arduino-sd-card-example.php.

45. **Schaad, J.** *Advanced Encryption Standard (AES) Key Wrap Algorithm.* místo neznámé : RSA Laboratories, 2002.

46. **Karri, Bo Yang Kaijie Wu Ramesh.** *Scan Based Side Channel Attack on Dedicated Hardware Implementations.*

47. **Sigfox.** *Oživujeme věci.*

48. Sigfox-tutorial. *RF wireless.* [Online] http://www.rfwireless-world.com/Tutorials/Sigfox-tutorial.html.

49. Arduino power consumption. *Learn Sparkfun.* [Online] https://learn.sparkfun.com/tutorials/reducing-arduino-power-consumption.

Seznam obrázků

Seznam tabulek

Seznam symbolů, veličin a zkratek

OTP	One Time Pad (Vermanova šifra)
AES	Advanced Encryption Standart
DES	Data Encryption Standart
IoT	Internet of Things
CRC	Cyclic Redundancy Check
M2M	Machine 2 Machine
BTS	Base station (Základnová stanice)
VSWR	Volatage Standing Wave Ratio
UNB	Ultra Narrow Band
LBT	Listen Before Talk
AFA	Adaptive Frequency Agility
SSL	Secure Sockets Layer
ČTÚ	Český telekomunikační úřad
IV	Inicializační vektor
XOR	Exclusive Or
GPS	Global Positioning System

Seznam příloh