

---

# **Cybersécurité, initiation au binôme HackRF One et Universal Radio Hacker**

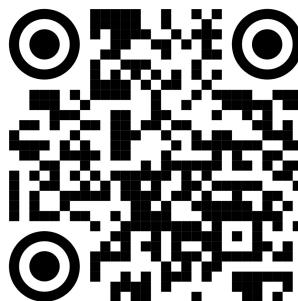
*Autrement dit « SéSAME, ouvre-toi... », quelques trésors  
technologiques dévoilés*

***Exemple d'une clé électronique sans-fil  
qu'on imagine « sécurisée »***

---

*Ce document est publié au format PDF sur mon blog.*

*Pour s'y rendre, scannez ce QR-Code ou rendez-vous ici : <https://pchene.wordpress.com/>*



*Ce document tout comme le contenu de mon blog est libre de diffusion dans un cadre non-rémunéré.  
Dans le cas contraire, merci de me solliciter afin d'obtenir ou pas une autorisation écrite. Il s'en suivra  
un échange ou j'apprécierai vos motivations. Mon autorisation ou pas en sera ma conclusion.*

*Un cadre rémunéré étant un cadre dans lequel votre activité de diffuser intégralement ou  
partiellement mon contenu est susceptible de produire un gain financier, une contrepartie de toute  
nature (salaire, dédommagement, cadeau...)*

*Pour me contacter : [14VK11@gmail.com](mailto:14VK11@gmail.com)*

## Table des matières

Introduction.....	4
Les solutions techniques utilisées .....	6
Clé SDR (RTL-SDR) ou HackRF ? .....	7
L'aspect logiciel .....	8
Universal Radio Hacker, l'outil cybersécurité des systèmes communicants sans fil .....	8
Satsagen, l'analyseur de spectre... .....	9
Ça sert à quoi un analyseur de spectre ? .....	9
Bien plus qu'un Analyseur de Spectre.....	10
Mise en route du système télécommandé .....	11
Une transmission radio, 2 notions fondamentales .....	12
La fréquence d'émission.....	12
La modulation.....	12
Comment identifier la fréquence d'émission de la clé ?.....	13
Le logiciel Satsagen.....	13
Mise en route de Satsagen.....	14
Paramétrage de l'analyseur de spectre.....	15
Universal Radio Hacker : Configuration .....	17
Universal Radio Hacker et son outil « Spectrum Analyser » .....	18
Informations à retirer de cette observation .....	20
Que devrait-on avoir comme modulation ?.....	21
Universal Radio Hacker : Enregistrer et observer .....	22
La modulation.....	28
La modulation ASK.....	31
La modulation OOK .....	31
Emettre un signal .....	35
Emettre, des précautions pour éviter la casse.....	35
Réaliser une charge fictive .....	37
Emettre le signal enregistrer .....	38
Autopsie de la clé .....	40
Conclusions.....	44
Conclusion sur le HackRF.....	44
Conclusion sur la suite logicielle Universal Radio Hacker .....	44
Conclusion sur cette faille du système de télécommande.....	44
Sans verser dans la paranoïa mais à méditer .....	45

Pour aller plus loin.....	46
Initiation aux modulations numériques et codages.....	46
Quelques usages du HackRF One .....	46
Cybersécurité et communication sans fil .....	46
A l'écoute des signaux numériques.....	47
Quelques points de contraintes et/ou obligations sur les radios transmissions .....	48

## Introduction

Cet article présente des outils, méthodes et retours d'expériences qui permettent d'aborder le sujet de la sécurité des clés sans fil de commande de nombreux systèmes d'ouverture/fermeture qui occupent nos environnements quotidiens.

Merci beaucoup à Pierre pour sa relecture, son regard différent et compétent en amont de la publication de ce document.

Initialement, j'ai conçu l'animation des activités présentées ici pour mon fils Viktor (14 ans). Il est passionné d'informatique, d'électronique, de robotique depuis tout petit. Dès ses 3 ans, je n'avais plus accès aux tablettes de la maison et il réalisait ses premiers kits d'électronique (robotique, radio...) dès l'âge de 6 ans. Il rêve actuellement de devenir ingénieur en Cybersécurité. La suite de ce document est une synthèse des activités que nous avons menées ensemble durant ces vacances de Noël 2024.

Par un exemple simple mais avec des outils performants de cybersécurité, je présente comment contourner la sécurité, avec succès et méthode, une clé et son boîtier de commande qu'on imagine pourtant « sûre ».

Pour illustrer cette activité de hacking, j'ai utilisé une clé sans fil et son boîtier de commande qu'on retrouve dans de nombreuses applications domestiques. Elle permet d'aborder en douceur cet univers des commandes sans-fil numériques.

Il est possible de poser un regard en lien avec des activités malveillantes sur les termes de « hack », et ses dérivés pour autant c'est aussi un pan légale des activités de sécurité, de recherche, d'enseignement... Associer hacking, hacker, hack à l'unique monde du crime est une vision biaisée de la réalité. C'est l'intention, l'usage de ce que vous ferez des connaissances, méthodes, outils acquis qui feront de vous un criminel au regard des lois qui régissent notre/nos société(s). Ce document n'est donc pas publié dans l'intention de faciliter des activités criminelles. Il a une vocation pédagogique pour comprendre quelques principes de base de ces systèmes sans fil.

Le modèle de clé et « serrure » choisi pour illustrer ce document correspond à celui-ci, son prix (clé + boîtier de commande) est d'environ 13 euros : <https://amzn.to/41VWNYT>



Ces systèmes radiocommandés se retrouvent souvent sur des portails de jardin, ou pire sur des portes de garage automatisées dont le garage donne sur un intérieur de maison ... et c'est à mon sens un problème car un grand nombre d'entre nous s'imagine faussement en sécurité parce que cela s'appelle « clé » et que ça ressemble à une clé de voiture (un peu plus sécurisé et pourtant là aussi...)

Pour les fans inconditionnels de solutions quasi prêtées à l'emploi, vous allez être probablement déçus par ce qui va suivre car ici le but n'est pas de verser dans le copier/coller mais de comprendre ce qu'il se passe.

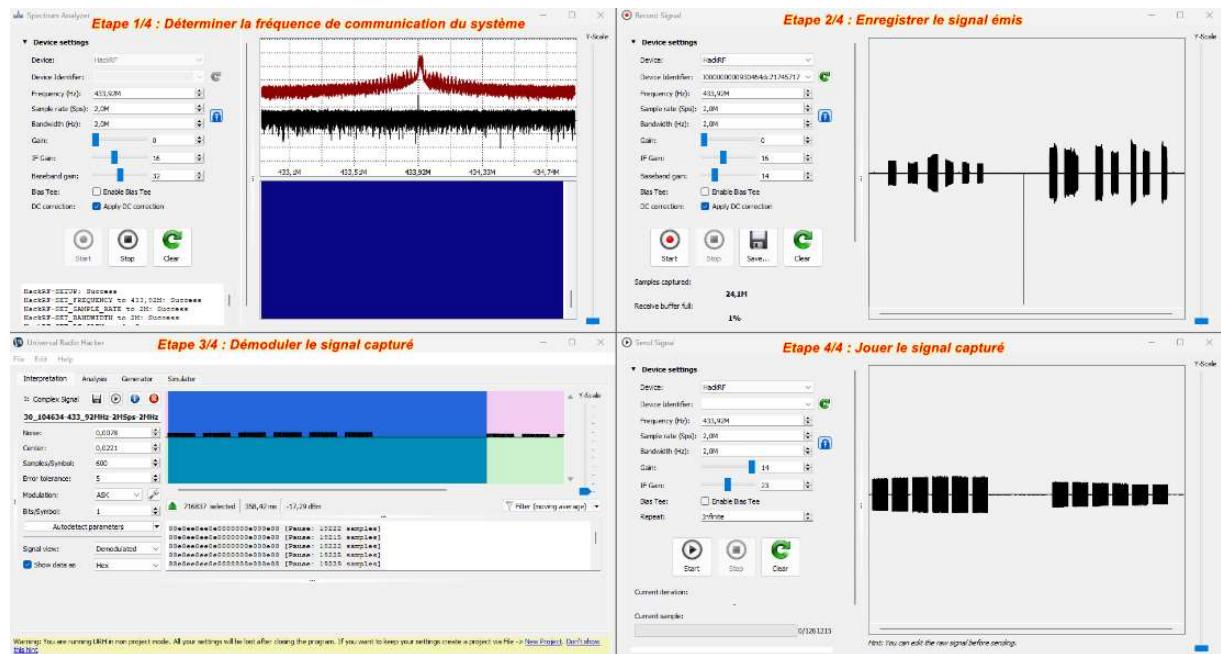
Bien évidemment la suite logicielle Universal Radio Hacker permet, elle aussi, de se limiter au « Replay » dénué d'agitation pour les neurones (Etapes 2 et 4 sur la copie d'écran ci-dessous), disponible sur ces outils que sont les FlipperZero, EvilCrowRF, Portapack et d'autres.

Ma volonté est de proposer ici des éléments de compréhension afin d'aller au-delà de nombreux contenus présentés par certaines vidéos (tutos), blog... qui traînent sur Internet et qui stagnent sur une démonstration du « Replay » sans prendre le temps de présenter quelques concepts fondamentaux d'une communication numérique ou pas sans fil.

Il est évident que si à la suite de la parution de ce document Mamie se fait dérober ses Louis d'Or dans le bas de laine caché sous le tapis du teckel. Sans vous raconter de salades, je peux affirmer que je n'en suis nullement responsable ou coupable (voir les éléments de langage d'une célèbre ministre française).

Fidèle à mon habitude, je propose de nombreux liens (en bleu) qui permettront à celui qui le souhaite d'approfondir une multitude de sujets liés à ce contenu. Ce document est une porte d'entrée dans l'univers de la cybersécurité et n'est nullement une fin en soi.

Il s'articule autour des 4 étapes suivantes :



## Les solutions techniques utilisées

J'ai utilisé le matériel suivant pour mener l'observation et l'attaque de la télécommande :

- Un PC sous Windows 11, un PC sous Windows 7 peut aussi être utilisé, j'utilise régulièrement une telle solution avec les logiciels présentés ici. Si on se limite à l'utilisation de la suite logicielle URH pour exploiter un HackRF, on peut tout à fait utiliser d'autres OS.
- Un HackRF One (appelé souvent HackRF) qui vient de chez Aliexpress. Il est possible aussi d'utiliser un Portapack en se rendant dans son menu « HackRF ».

Le HackRF One fabriqué en Chine est normalement à l'identique de l'original car les différents plans, PCB et logiciel (firmware) sont libres de diffusion (<https://github.com/greatscottgadgets/hackrf>) donc on ne peut pas parler de copie ou contrefaçon comme j'entends ou lis régulièrement.

Je rappelle que « The mission of Great Scott Gadgets is to put open source tools into the hands of innovative people. » et c'est écrit ici, par eux :

<https://greatscottgadgets.com/opensource/>

Pour disposer de plusieurs HackRF venant de cette plateforme d'e-commerce chinoise (payé moins de 84 euros encore récemment, novembre 2024) ils fonctionnent parfaitement même après une mise à jour (ah certains arguments...) alors pourquoi payer bien plus cher chez des revendeurs français (autour de 350 euros) ou autres ? L'intérêt de l'acheter au concepteur ou à son revendeur officiel est un autre débat mais ne joue normalement en rien sur les performances du HackRF One.

J'ai utilisé au cours de la rédaction de document une version 10 avec un Portapack H2+, une version 9 seule et même une version de 2014. Les deux logiciels mentionnés ci-après n'en n'ont pas été troublé.

- Le logiciel Satsagen qui permet d'utiliser le HackRF comme un analyseur de spectre mais pas que. Si vous ne le connaissez pas, mon ambition est de vous faire découvrir cette très belle réalisation qui est gratuite dans le cadre d'un usage non-commercial.
- Et enfin, la suite logicielle Universal Radio Hacker qui est gratuite sur laquelle repose l'intégralité de cette expérience.

## Clé SDR (RTL-SDR) ou HackRF ?

Il est possible de reproduire partiellement les manipulations exposées dans ce document avec une Clé SDR. Mais je dis bien partiellement, car celle(s)-ci pour l'immense majorité (RTL-SDR) ne sont pas capable de passer à l'émission pour mener à bien l'attaque. Par contre pour toutes les étapes en amont, elles devraient fonctionner. Vous pourrez les utiliser avec Satsagen comme avec Universal Radio Hacker pour observer les signaux.

La différence de prix entre un HackRF dont le prix débute autour de 85 euros et une clé SDR premier prix, autour de 25 euros, tient entre autres dans le fait que cette dernière n'intègre pas la fonction émission.

La différence ne s'arrête pas là : Le HackRF a un span affichable à l'écran pouvant aller jusqu'à 20 MHz, l'émission et la réception vont jusqu'à 6GHz... voir jusqu'à 7GHz en analyseur de spectre avec le span de la même largeur 😊 (voir les liens sur le HackRF dans le chapitre « Pour aller plus loin »).

Si vous êtes amené à réaliser des expérimentations dans le domaine des radiofréquences, il est à mon sens bien plus avantageux de se procurer un HackRF qu'une clé SDR de type RTL-SDR.

En effet, le HackRF pour un passionné de radiofréquences aura de nombreuses autres applications, on peut citer rapidement :

- Les mesures
  - Analyseur de spectre
  - SNA (Scalar Network Analyser)
  - VNA (Vector Network Analyser)
  - Générateur RF,
  - ...
- Les activités de radio amateurisme à l'émission comme à la réception (Satellite QO 100, SWL...)
- Les activités de Maker
- Les activités de développement sous GNU Radio (<https://www.gnuradio.org/>) ce qui ouvre la porte à la réalisation d'un banc d'essai, d'équipement RF sur mesure...
- Les activités relevant du cadre de la cybersécurité, du hack
- ...

De plus, le HackRF permet de recevoir le Portapack, une carte avec son firmware qui permet d'utiliser le HackRF sans PC. Le Portapack, intègre de nombreux outils de hack comme on peut trouver sur l'outil Flipper Zero mais il ne s'arrête pas à cela (ouf !). Tout comme le HackRF, il est disponible sur Aliexpress ... à un prix agréable. L'ensemble est compact, tient dans la main et intègre écran tactile, batterie, un HP, un connecteur micro et casque... Et il est toujours possible d'utiliser le combiné (portapack/hackRF One) comme un simple HackRF car c'est prévu par le firmware. C'est d'ailleurs ce que je fais avec deux des miens selon le besoin d'usage.

Pour le Portapack, à voir ici <https://github.com/portapack-mayhem/mayhem-firmware> et ici aussi <https://hackrf.app/>

## L'aspect logiciel

Je vais aborder l'usage de 2 outils logiciels gratuits et particulièrement appréciables dans le cadre du hack de systèmes communicants par onde radio. Ils sont d'une prise en mains aisée par l'utilisateur qui est initié ou formé aux techniques, mesure... de leurs domaines d'usage. Ils sont disponibles ici :

- Universal Radio Hacker : <https://github.com/jopohl/urh>
- Satsagen : <https://www.albfer.com/en/2020/02/21/satsagen-2/>

### **Universal Radio Hacker, l'outil cybersécurité des systèmes communicants sans fil**

Universal Radio Hacker ou aussi appelé URH est une suite logicielle open-source qui n'a pas de concurrence en l'état de mes connaissances. Elle est conçue pour l'analyse de protocole, elle permet un flux de travail complet en proposant un travail intuitif sur :

- La démodulation des signaux,
- Les décodages personnalisables,
- Une prise en charge du fuzzing (technique de test de sécurité automatisé qui consiste à envoyer des données invalides, aléatoires ou inattendues dans un système informatique),
- La réalisation de simulations.

URH divise le processus en des étapes d'interprétation, d'analyse, de génération et de simulation, grâce auxquelles les résultats d'une étape peuvent être transférés à l'autre. Le logiciel offre toutes les fonctionnalités nécessaires à l'investigation du protocole sans submerger les utilisateurs de complexité.

URH a été initialement développé à l'intention des chercheurs qui souhaitent se concentrer sur la logique du protocole et essayer d'éviter de plonger dans les profondeurs du traitement du signal HF et numérique. Mais sa simplicité d'usage en fait aussi une excellente solution pour l'amateur de signaux numérique.

Cette suite peut être utilisée avec la plupart des plateformes de développement SDR (radio définie par logiciel) tel que le HackRF One mais pas que. URH est gratuit, disponible sous Windows comme sous Linux et même sur macOS, donc le « rêve » car c'est loin d'être toujours le cas sur les outils de ce type 😊.

Ici quelques points qui sont à mon sens bien sympathiques dans cette suite logicielle en plus de ces aspects fonctionnels intrinsèques :

- URH reconnaît les clés RTL-SDR (attention uniquement de la réception est possible).
- URH est régulièrement mis à jour et évolue fonctionnellement.
- URH ravira les possesseurs de l'outil Flipper Zero car cette suite logicielle permet d'exporter les fichiers vers cet outil (<https://flipperzero.one/>)
- URH trouvera tout aussi des utilités pour construire des attaques avec l'outil au hardware programmable EvilCrowRF-V2. Pour ce dernier, ces trois liens sont un début de compréhension :
  - <https://github.com/joelsernamoreno/EvilCrowRF-V2>
  - [https://youtu.be/TAgtaAnLL6U?si=O-IJubO3FI\\_6mCYL](https://youtu.be/TAgtaAnLL6U?si=O-IJubO3FI_6mCYL)
  - [https://github.com/h-RAT/EvilCrowRF\\_Custom\\_Firmware\\_CC1101\\_FlipperZero](https://github.com/h-RAT/EvilCrowRF_Custom_Firmware_CC1101_FlipperZero)

J'ai tendance à penser que Universal Radio Hacker est actuellement l'outil à posséder pour investiguer les protocoles sans fil qui envahissent notre quotidien (clés, objets connectés divers et variés). Associé à la plateforme de développement SDR HackRF One, on a là une solution efficace et à faible coût pour jouer ou pas dans la cour des grands 😊.

Ici, vous avez un document PDF plutôt complet qui le présente :

<https://www.usenix.org/system/files/conference/woot18/woot18-paper-pohl.pdf>

## Satsagen, l'analyseur de spectre...

Ça sert à quoi un analyseur de spectre ?

Satsagen est un logiciel d'analyse du spectre RF (SA – Spectrum Analyzer) qui offre aussi la possibilité d'être un générateur de signaux RF quand la carte le permet. En combinant ces deux fonctions, on peut alors obtenir d'autres appareil de mesure comme un analyseur de réseau scalaire (SNA – Scalar Network Analyzer) puis Satsagen va encore plus loin car il est possible de l'utiliser en tant qu'analyseur de réseau vectoriel (VNA – Vector Network Analyzer). Ils ne sont pas comparables à leurs grands frères dont le prix est de plusieurs milliers d'euros voir bien plus, pour autant ils peuvent rendre de grands services à l'amateur.

Un analyseur de spectre permet d'afficher un spectre de fréquences plus ou moins large et d'en observer son amplitude. C'est l'outil de mesure « de base » de toute personne qui a une activité dans le domaine des radiofréquences. Dans la littérature, on retrouve cette définition : Un analyseur de spectre est un instrument de mesure destiné à afficher un signal dans le domaine fréquentiel.



Vous connaissez peut-être l'oscilloscope. Ce dernier affiche le signal dans le domaine du temps. L'abscisse (axe horizontal du graphe) étant le temps et l'ordonnée (axe vertical du graphe) est la représentation de l'amplitude du signal. Donc l'oscilloscope représente l'évolution de l'amplitude du signal dans le temps.

Dans le cas de l'analyseur de spectre, l'abscisse représente les fréquences et l'ordonnée c'est la représentation de l'amplitude du signal comme pour l'oscilloscope. Donc l'analyseur de spectre

représente l'évolution de l'amplitude d'une ou de fréquences dans un spectre de fréquences donné. Ce spectre de fréquences donné est nommé le « Span », il est donc délimité par une fréquence minimum et une fréquence maximum. Cette amplitude, peut être en représentée dans les différentes formulations du gain mais aussi en tension, puissance...

Quand une émission a lieu dans le spectre de fréquence choisi alors un ou des pics apparaissent à l'écran. Si le span visualisé est suffisamment large, on pourra alors visualiser les différentes harmoniques du signal émis.

### *Bien plus qu'un Analyseur de Spectre*

Le logiciel Satsagen est avant tout une caisse à outils pour mener des analyses sur le spectre de radiofréquences. Il propose de se connecter à de multiples équipements courants de type « analyseur de spectre » ou SDR que ce soit sous la forme de carte, boîtiers ou clés.

Je l'utilise avec succès avec le HackRF, différentes clés RTL-SDR, la carte D6 JGP-1033, un HamGeek Radio SDR (PIAA+)

Le HackRF offre avec Satsagen un ensemble en mesure de « travailler » jusqu'à 6 GHz avec un span lui aussi pouvant aller jusqu'à 6 GHz 😊. Et bien entendu, son générateur de signaux RF permet lui aussi de monter jusqu'à 6 GHz.

Parmi les outils qu'il offre à ce jour, il y a ceux-ci et cette liste n'est pas exhaustive :

- Un analyseur de spectre dont la gamme de fréquence est limité par périphérique... Avec le HackRF One, il est alors possible de faire des mesures jusqu'à 6GHz ce qui est imposant pour la plupart des amateurs.
- Un générateur de signaux RF qui offrent de multiples modulations dont des modulations fournies par l'extérieur (sous forme de fichier).
- Un outil SNA
- Un outil VNA
- Un démodulateur radio avec les modulations courantes comme l'AM, différentes FM, la BLU
- L'utilisation de marqueurs divers et variés
- Le Waterfall ou chute d'eau
- Des mesures de Noise Figure et de Gain
- Des mesures d'ENR
- Des mesures de déviation en AM, FM et SSB
- Différentes mesures pour les modulations AM et FM
- La possibilité d'y connecter un GPS

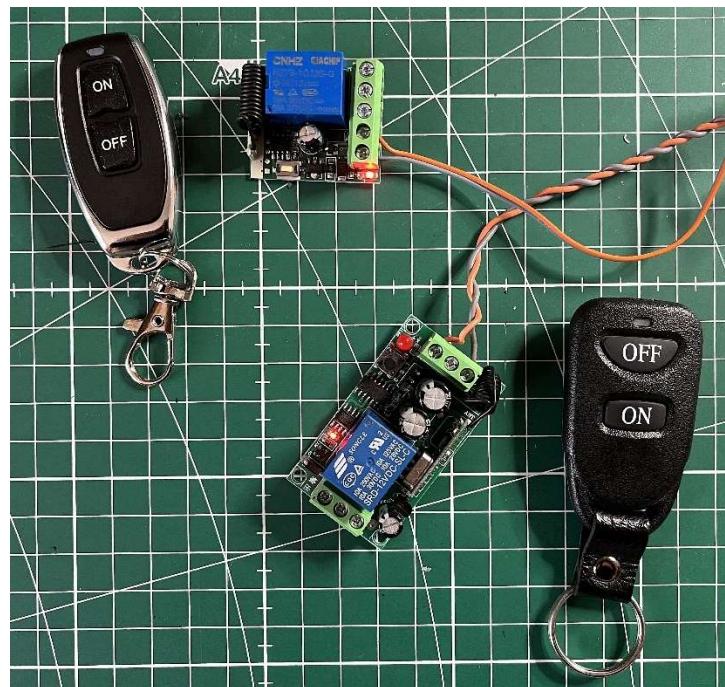
Ce logiciel est régulièrement mis à jour (corrections et évolutions). Des vidéos existent à son sujet sur Youtube... Globalement, elles sont anciennes et sont donc en retard sur l'étendue de ses possibilités.

La page de son développeur mérite d'être visitée pour se faire une idée de ses possibilités de manière plus approfondie :

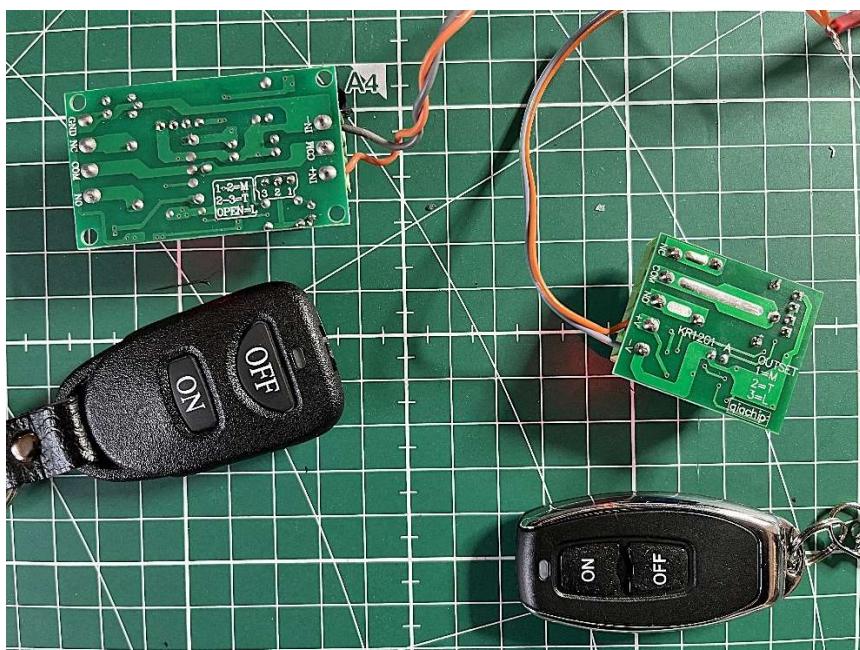
<https://www.albfer.com/en/satsagen-topics-index/>

## Mise en route du système télécommandé

Les modèles utilisés sont très courants. En cliquant sur les boutons de la clé, sur mes modèles, une LED soudée sur le PCB change d'état (éteinte, allumée). Sur la photo ci-dessous, elle est rouge. J'ai dans mon stock une clé plus ancienne, à part les dimensions plus importante, tout est identique dans le fonctionnement. On voit ci-dessous les deux :



A l'aide de la photo ci-dessous, il devrait être aisément de le connecter à une alimentation 12V afin de l'alimenter correctement. J'ai une vieille habitude de torsader les fils d'alimentation quand ceux-ci ne sont pas, d'origine, maintenus parallèles. Ce qui a pour effet de réduire la circulation du bruit. Mais ça n'a rien d'obligatoire ici.



## Une transmission radio, 2 notions fondamentales

Une transmission pour faire transiter une information utilisant les ondes radio s'appuie sur 2 notions :

- La fréquence,
- La modulation.

### La fréquence d'émission

La fréquence d'émission étant, la fréquence sur laquelle l'émetteur émet et donc sur laquelle le récepteur devra être réglé pour recevoir cette émission.

Cette fréquence est parfois appelée canal. Cette appellation « Canal » permet de simplifier entre autres l'usage d'un équipement.

Par exemple le canal 8 d'un équipement PMR446 correspond à la fréquence 446,09375 MHz. Il est donc plus simple et rapide d'annoncer à son correspondant de se rendre sur le numéro du canal que d'annoncer la fréquence pour établir la communication. Puis du coup, pour le concepteur de l'équipement, l'affichage de la fréquence s'en trouve simplifié.

*Figure 1 : Ici un exemple d'usage de la notion de canal avec un talkie-walkie spécifique réglé sur le canal 16 de la bande VHF Maritime. La fréquence correspondante au canal 16 de la VHF Maritime est la suivante : 156,800 MHz*



### La modulation

La fréquence permet de transporter une voix, un message numérique, un son.... Pour réaliser cela, il faut alors installer la donnée (voix, donnée numérique, son...) dans un « véhicule » qui va permettre de transporter celle-ci sur la fréquence d'émission.

A l'émission, il va falloir **moduler** la donnée à transporter sur la fréquence d'émission. A la réception, il est alors de nécessaire de procéder à l'opération inverse. C'est-à-dire le récepteur, va **démoduler** la donnée à recevoir.

Donc, on a : Un émetteur module et un récepteur démodule la donnée transmise.

Ce qui implique que le récepteur doit utiliser la même modulation employée par l'émetteur pour pouvoir reproduire la donnée.

Pour une télécommande sans fil, un objet connecté... tout ceci est aussi valable. Les prochains chapitres posent les principes de base pour identifier la fréquence de transmission par plusieurs moyens. Puis le sujet de la modulation sera abordé ainsi que le type de modulation spécifique couramment employé par les concepteurs de ce type de solution pour transporter la donnée vers l'équipement à mettre en action (portail, porte de garage, éclairage ...). Et bien évidemment, le document expose comment observer l'information contenue dans la modulation afin de la traiter pour une reproduction, modification, compréhension...

## Comment identifier la fréquence d'émission de la clé ?

Des fréquences, il en existe, à priori, sans fin. Pour notre clé ou d'autres systèmes de communication, comment identifier la bonne fréquence dans cet infini peut-être un moment de grande solitude ou une interrogation obstacle ou frein pour aller plus loin.

L'usage des fréquences est réglementé au niveau international puis par pays mais aussi par des conglomérats d'états comme par exemple l'Europe.

Dans notre cas, pour un usage libre par le plus grand nombre d'usagers, ceci conduit les fabricants de ces objets radio à utiliser des fréquences dites ISM (industriel, scientifique et médical). Les bandes de fréquences ISM ne sont pas si nombreuses, ce qui va nous faciliter la tâche, voir ici par exemple :

- [https://fr.wikipedia.org/wiki/Bande\\_industrielle,\\_scientifique\\_et\\_m%C3%A9dicale](https://fr.wikipedia.org/wiki/Bande_industrielle,_scientifique_et_m%C3%A9dicale)
- [https://learninglab.gitlabpages.inria.fr/mooc-iot/mooc-iot-ressources/Module1/S02/C034AA-M01-S02-part1-cours\\_FR.html](https://learninglab.gitlabpages.inria.fr/mooc-iot/mooc-iot-ressources/Module1/S02/C034AA-M01-S02-part1-cours_FR.html)

Cette fréquence n'a donc rien de « secrète », elle n'est pas un mystère. De plus, le fabricant est obligé (théorie) de déclarer la ou les fréquences d'émission donc en sachant cela, c'est plutôt simple de retrouver l'information. Bien souvent pour l'obtenir, il suffit de lire l'intitulé du produit ou sa notice.

Une autre solution, si le produit est distribué aux USA, ce qui est souvent le cas, et si le fabricant a rempli ses obligations déclaratives, il suffit de consulter la base de données de la FCC ( Federal Communications Comission - <https://www.fcc.gov/> ). Pour cela, vous regardez l'étiquette ou gravure en général au dos de l'équipement et vous repérez l'identifiant FCC-ID puis vous le saisissez dans le lien suivant : <https://fccid.io/>

Comme vous le verrez, vous avez alors accès à un tas de documents sur le produit concerné en plus de sa ou ses fréquences. On y trouve normalement aussi les manuels utilisateurs, ce qui peut être utile parfois.

D'autres moyens existent pour déterminer la fréquence d'émission d'un produit. En voici un, plus technique, qui consiste à utiliser par exemple le HackRF One en analyseur de spectre grâce au logiciel Satsagen ou un autre.

### Le logiciel Satsagen

La fonction « Spectrum Analyser » du logiciel Universal Radio Hacker est capable de satisfaire à notre recherche de fréquence de la clé. Mais ici c'est surtout l'occasion, pour ceux qui ne le connaissent pas, de présenter ce logiciel qui est une solution permettant d'obtenir plusieurs équipements importants pour « travailler » dans le domaine des radiofréquences.

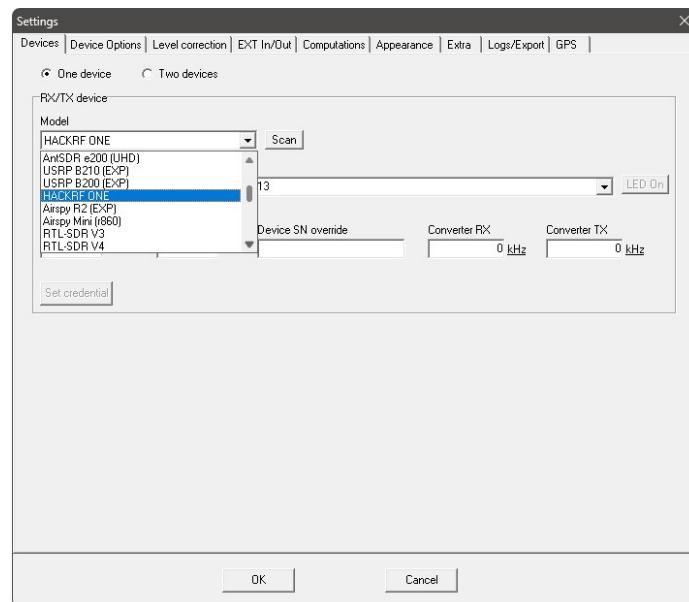
Un électronicien... qui souhaite élargir ses compétences dans le domaine des radiofréquences trouvera rapidement la nécessité de posséder un analyseur de spectre et un générateur de signaux HF. Pour celui qui se lance dans la cybersécurité des systèmes sans fil, ces 2 équipements deviennent aussi rapidement indispensables.

Voyons donc ce que satisfait Satsagen au lieu d'utiliser la fonction « Spectrum Analyser » du logiciel Universal Radio Hacker.

## Mise en route de Satsagen

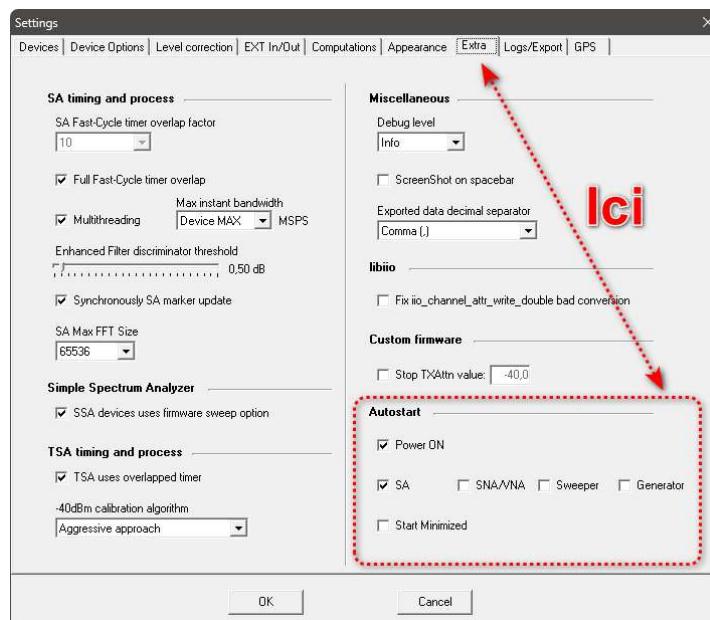
Une fois Satsagen lancé, rendez-vous dans le menu « Settings » puis « More settings... ».

Il faut au préalable déclarer dans l'onglet « Devices » votre HackRF ou un autre des équipements acceptés. Si vous êtes dans un contexte où il n'y a qu'un unique équipement utilisé alors vous n'aurez rien de plus à faire, sinon il vous faudra cliquer sur « Two devices » et déclarer le second équipement.



Avec le HackRF ou un autre périphérique déclaré, je vous propose de vous rendre dans l'onglet « Extra » afin que le logiciel Satsagen démarre en mettant en route l'analyseur de spectre automatiquement. Ce qui évite à chacune de ses utilisations de devoir cliquer sur le bouton carré « Power » en bas et à gauche de l'écran puis sur celui, en haut et à droite, appelé « Spectrum Analyser ».

Pour réaliser cela, dans la partie « Autostart » de cet onglet, vous cochez alors « Power ON » et « SA » comme indiqué dans la copie d'écran suivante :



## Paramétrage de l'analyseur de spectre

Pour la suite, il faut donc considérer que la bande de fréquence est très probablement de l'ISM car sinon il y a la problématique des contraintes de réglementation limitantes pour le fabricant comme pour l'utilisateur du système de la télécommande. En Europe, les différentes bandes ISM sont les suivantes :

- En HF
  - 6,765 à 6,795 MHz
  - 13,553 à 13,567 MHz
  - 26,957 à 27,283 MHz
- En VHF
  - 40,660 à 40,700 MHz
- En UHF
  - 433,05 à 434,79 MHz (selon autorisations nationales)
  - 2,4 à 2,5 GHz
- En SHF
  - 5,725 à 5,875 GHz
  - 24,0 à 24,25 GHz
- En EHF
  - 61,0 à 61,5 GHz
  - 122,0 à 123,0 GHz
  - 244,0 à 246,0 GHz

Contourner la sécurité des systèmes de communication sans fil dans la bande EHF nécessite des savoirs faire et des moyens plus onéreux. Pour faire simple, c'est réservé à certains professionnels ou des amateurs particulièrement avertis. Les bandes HF, VHF, UHF et la première bande de fréquences en SHF sont plus simplement accessibles surtout depuis l'avènement des équipements SDR comme le HackRF, Pluto... sans parler des modules spécialisés sur tel ou tel bande de fréquences.

Plus la fréquence est basse plus sa longueur d'onde est grande. La longueur d'onde s'exprime en mètre tout comme quand on mesure une dimension. Ce qui engendre une antenne plus ou moins encombrante. Pour un produit qui se doit d'être discret et pour lequel il faut garantir une portée autre que de coller l'émetteur au récepteur, il est donc préférable d'utiliser une longueur d'onde raisonnable.

Voici quelques grandeurs de longueur d'onde :

- 3 MHz c'est 100 m
- 30 MHz c'est 10 m
- 300 MHz c'est 1 m
- 3 GHz c'est 10 cm
- 30 GHz c'est 10 mm
- 300 GHz c'est 1 mm

$$\text{Avec : Longueur d'onde en mètre} = \frac{300}{\text{Fréquence en MHz}}$$

Donc 10 m de longueur (à 30 MHz) ça commence à faire surtout quand il faut loger cela dans un si petit boîtier de télécommande et pouvoir assurer une portée d'une cinquantaine de mètre ou un peu plus. Rappelez-vous les dimensions d'une antenne cibi sur un toit (27 MHz), c'est visible de loin. Oui on peut toujours raccourcir une antenne (par exemple dans les systèmes RFID) par certaines

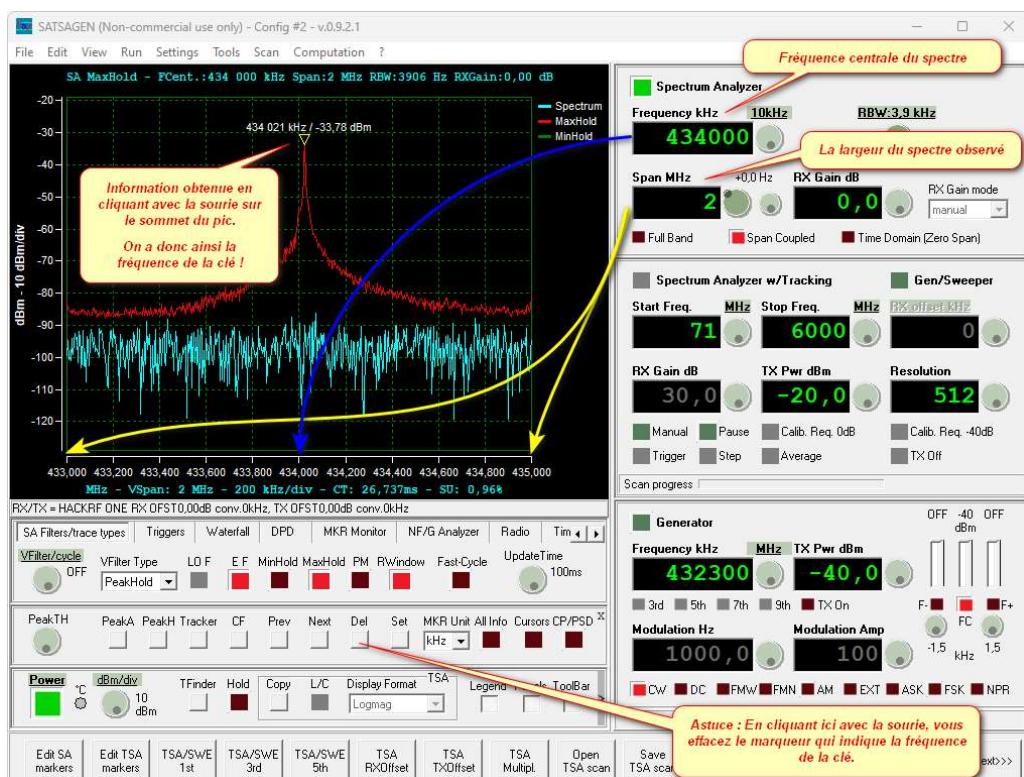
techniques mais il y a des limites existantes difficilement franchissables dans l'état actuel du savoir pour assurer un minimum de portée utile.

Ici, dans le cas de cette clé, les bandes ISM HF et VHF ont peu de chance d'être utilisée. Il nous reste naturellement les bandes UHF et éventuellement SHF. Donc très naturellement, la bande ISM UHF mérite d'être explorée avec l'analyseur de spectre, elle est comprise entre 433 MHz et 435 MHz. Elle est aussi appelée la bande ISM 433 et nous donne sensiblement une longueur d'onde de 69 cm. Et là tout devient plus simple pour loger l'antenne dans le boîtier pour le constructeur et obtenir une portée de transmission satisfaisante.

Avec l'analyseur de spectre, nous allons pouvoir vérifier cette hypothèse (ISM 433) en le réglant sur cette bande de fréquences. Si c'est le cas nous verrons un pic important apparaître sur son graphe au moment où l'on enfonce un des boutons de commande (ON/OFF ou A/B ou ...) de la clé.

Le réglage de l'analyseur de spectre est alors le suivant :

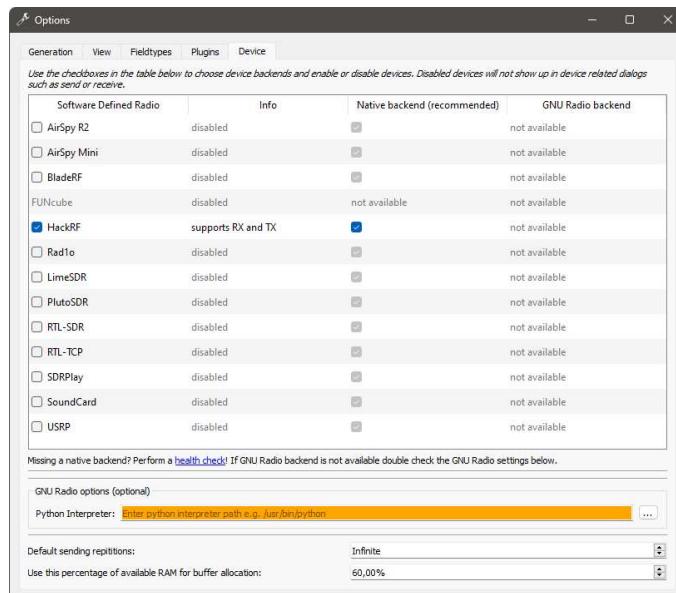
- Dans la partie « Spectrum Analyser » on peut régler la fréquence centrale du spectre à observer. Ici elle est affichée en KHz et elle est de « 434000 KHz ». Le Span ou la largeur de bande à observer sera réglé à 2 MHz ce qui permet de visualiser l'intégralité de la bande ISM 433 qui est répartie de sensiblement 433 MHz à 435 MHz. On a donc la fréquence de 434 MHz comme le milieu de cette bande, c'est donc plus pratique de centrer l'affichage. Tout signal émis dans cette bande de fréquences apparaîtra sous la forme d'un pic.
- Les différents boutons carrés et rouges, vous pouvez jouer avec pour en visualiser l'effet sur les graphes.
- Les parties relatives à « Spectrum Analyser w/tracking » « Gen/Sweeper » et « Generator » correspondent à d'autres instruments de mesures qu'offre ce logiciel. Ici, ils ne sont pas utilisés ici.



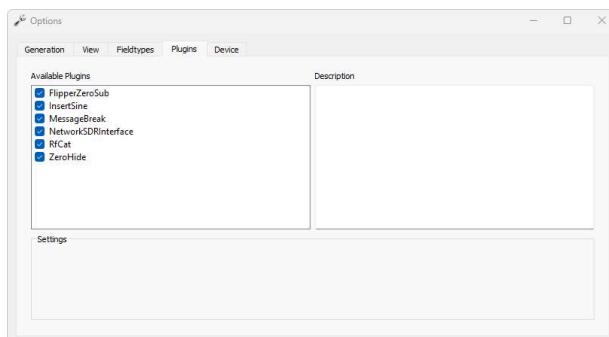
La trace rouge mémorise le signal quand j'enfonce (modérément) un des 2 boutons de la clé, la trace bleue est le signal en temps réel. En cliquant sur le bouton « MaxHold » ici en rouge, vous faites disparaître ou pas l'affichage de la trace en rouge. En haut du pic de la trace rouge est indiquée la valeur de la fréquence, soit quasiment 434 MHz dans mon cas (ma clé). Attention ici ce pic n'est pas la fréquence d'émission de la clé. Nous reparlerons de cela un peu plus loin après avoir introduit la notion de modulation. Ce pic à 434 MHz nous montre simplement que la clé émet à proximité de cette fréquence à quelques KHz près. Vous obtenez ce repère et sa valeur en présentant le curseur de la souris sur le sommet du graphique puis vous cliquez son bouton gauche (souris). Pour effacer un marqueur, il suffit de cliquer sur « Del » comme indiqué sur la copie d'écran précédente qui est commentée.

## Universal Radio Hacker : Configuration

Avant de lancer tel ou tel outil de la suite logiciel URH, il est préférable de passer par le menu « Edit » puis dans l'onglet « Options... », la fenêtre ci-dessous devrait s'afficher. Je vous propose de décocher les solutions périphériques que vous n'utilisez pas. Ce qui évite à chaque lancement d'URH de devoir sélectionner sa solution d'équipement SDR. Si vous n'avez que le HackRF One, alors on obtient ceci :



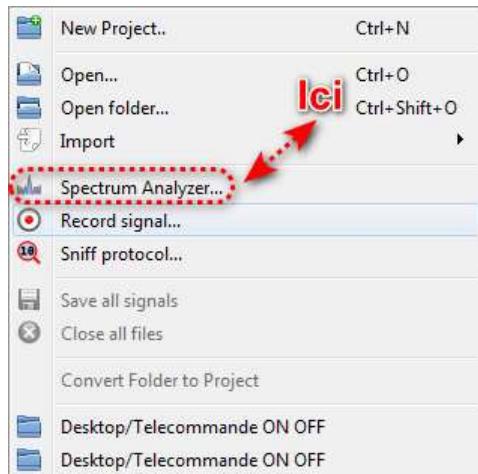
Tant qu'à être dans cette fenêtre, vous aurez peut-être un intérêt, en fonction de vos outils et besoins, à sélectionner les différents plugins indiqués ci-dessous en vous rendant dans l'onglet « Plugins » puis en cochant les cases qui vous conviennent. Dans le cadre de l'exemple de ce document ce n'est pas très utile :



## Universal Radio Hacker et son outil « Spectrum Analyser »

Avec la fonction « Spectrum Analyser » ou analyseur de spectre (facile la traduction) de la suite logicielle URH (voir menu « File »), on peut faire la même chose mais c'est beaucoup moins « sexy » et surtout moins puissant en possibilités que Satsagen mais pour ce genre de « travail simple » c'est à priori suffisant dans la très grande majorité des cas.

Dans le menu « File » c'est ici :



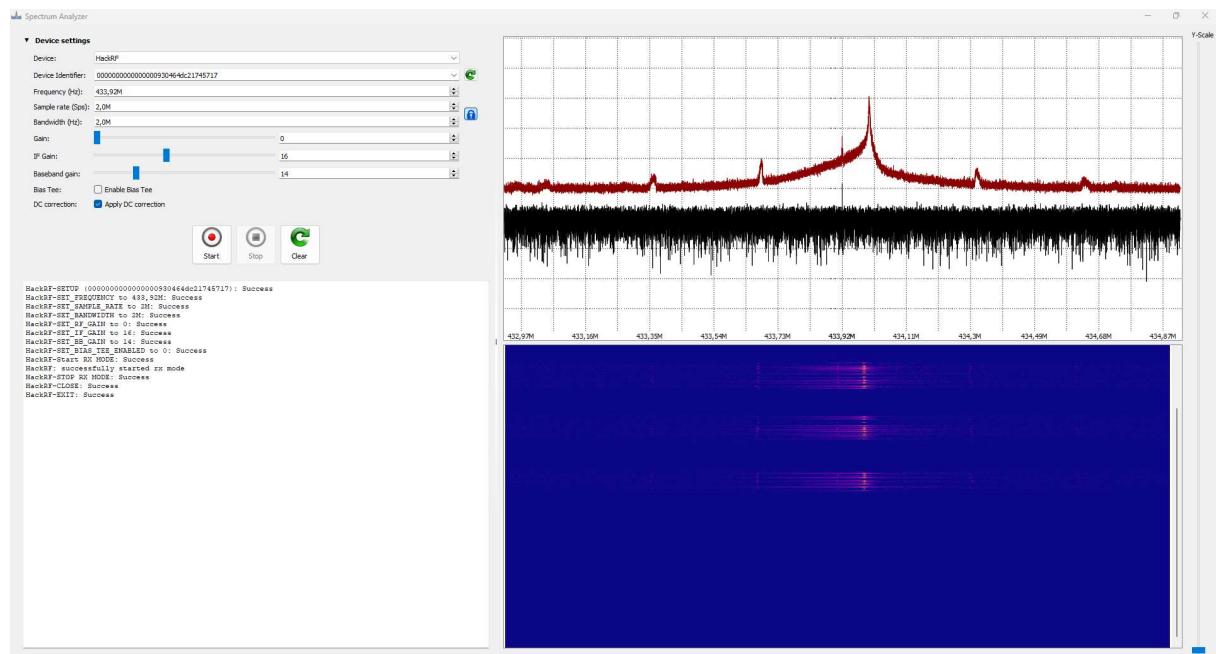
Voici ce que nous obtenons alors en respectant les paramètres que j'ai saisi :

- Soit notre fréquence de milieu de bande ISM 433 : 434 MHz pour « Frequency (HZ) ». En Europe, les clés de ce type sont normalement réglées pour émettre sur 433.92 MHz. Il est préférable de saisir cette fréquence.
- La bande passante à observer, soit 2 MHz nous devions observer de 433 à 435 MHz. C'est à saisir dans Bandwidth (Hz).
- Le Sample rate (Hz), soit le taux d'échantillonnage se règle automatiquement en fonction de la valeur de Bandwith (Hz). Bien entendu à condition que le cadenas (logo à droite) soit verrouillé.
- Le gain est à 0 et je vous conseille de le laisser, le préamplificateur (LNA) en entrée de l'étage de la réception sur de nombreuses versions de HackRF ne comporte aucune protection contre des signaux forts. Et il grille tout simplement si le signal reçu est trop fort. Même si le changer n'est pas une opération très compliquée pour celui qui sait dessouder et souder un composant CMS, ça reste toujours une opération « délicate ». Depuis quelque temps, une version Clifford du HackRF est vendue par certaines boutiques chinoises ou aussi appelée version R10, il est préférable de se procurer cette version car justement elle modifie ce problème de non protection de l'étage d'entrée du HackRF.
- Le « IF gain » à 8 et il n'est pas utile de dépasser une valeur de 16. Car 16 est une valeur normalement adaptée à l'étage « Fréquence Intermédiaire ». Cela évitera d'obtenir un signal non déformé par une saturation liée à un gain d'amplification trop important.
- Le « Baseband gain » à 8. Cette valeur est adaptée pour signaux proches comme ici un HackRF à proximité de la clé (manipulés sur le même bureau) ce qui évitera à nouveau une déformation du signal.
- Enfin Bias tee est décoché car cette fonctionnalité ne sert normalement à rien pour notre expérience. C'est une fonction qui sert à alimenter un équipement par le connecteur de l'antenne (préampli par exemple). A titre d'information vous trouverez ici un document qui

donne des explications plus complètes sur cette fonctionnalité qui n'est pas du tout spécifique au HackRF : <http://f6kht.free.fr/document/BiasT.pdf>

- Par contre DC correction est coché. Cette fonction offre la possibilité de retirer ou pas toute trace de la composante DC (continue) dans le signal à démoduler.

Il ne reste plus qu'à cliquer sur « Start » pour visualiser la trace qui devrait être ainsi :



Remarques :

- Quand vous saisissez une fréquence qui n'est pas un chiffre rond comme par exemple 434 MHz, il est important de placer une virgule et non un point comme séparateur. Bien entendu pour « K » s'il s'agit de « KHz » ou pour « G » s'il s'agit de « GHz » et rien s'il s'agit de « Hz ». Ex : 433,92M pour 433.92 MHz.
- Pour obtenir l'information de la fréquence sur le sommet du pic, pour cela il suffit d'y placer le curseur de la sourie.
- En rouge/bordeaux le signal maximum mémorisé et en noir le signal temps réel. Donc ce dernier passe à l'horizontale dès qu'on arrête d'appuyer sur l'un des 2 boutons de la télécommande. Sinon cela veut dire qu'il y a autre chose qui émet.
- Il est possible d'obtenir le Waterfall / Chute d'eau (la partie bleu et rose de cette copie d'écran) sur Satsagen, cela fait partie des nombreuses fonctions qu'il est possible d'afficher ou pas.

## Informations à retirer de cette observation

Le signal s'appuie sur une fréquence qui est la fréquence d'émission que nous venons d'identifier. Puis la modulation va transporter une information. Ici, elle n'est pas une voix comme en phonie mais elle est une donnée numérique. Il existe 4 grandes familles de modulations qui permettent de véhiculer une donnée numérique. Je vais en parler plus loin.

Sur un baby phone (par exemple en ISM 433 sans FHSS), on pourrait entendre grâce à la modulation, les pleurs de bébé ou le chat ronfler dans le lit de bébé 😊. Donc le principe important à retenir est similaire :

$$\text{Signal} = \text{Fréquence d'émission (ou réception)} + \text{Modulation}$$

Ici, cette modulation transporte un message entre la clé et le boîtier. La clé se comporte comme un dictateur (humour) et le boîtier exécute la donnée de clé sans aucune forme de remise en compte de l'ordre reçu à partir du moment où l'identifiant de la clé est reconnu. Il faut alors comprendre sans aucune forme de dialogue sécuritaire.

L'observation du spectre (analyseur de spectre), montre qu'aucun échange de données s'est mis en place entre la clé et le boîtier de commande une fois que l'un ou l'autre des 2 boutons de la clé est relâché. Seule la clé est bavarde, car il n'y a que le pic correspondant à la pression sur l'un des boutons qui apparaît sur le graphe temps réel (noir). Ce qui élimine un nombre important de solutions de sécurité dans ce système de télécommande.

Ceci confirme la logique « à moindre coût » de ce type de produit. Car il n'y a qu'une fonction émettrice dans la clé et seulement une fonction réceptrice dans le boîtier de commande. Donc un développement moins couteux, des essais moins onéreux, une intégration simplifiée dans les boîtiers, des composants moins complexes ce qui forcément a un impact sur les coûts, etc... Comme bien souvent la sécurité est sacrifiée au profit des marges, en usant de la crédulité, naïveté, confiance... des utilisateurs et c'est particulièrement vrai sur ce type de produit grand public.

Certains modèles de babyphones en sont aussi un autre exemple où la sécurité du contenu des communication n'est pas systématiquement considérée. L'utilisateur n'a pas implicitement le réflexe de l'éteindre (les deux parties) après le sommeil de bébé donc je vous laisse imaginer le contenu véhiculé librement quand celui-ci (l'émetteur) se trouve par exemple dans la chambre parentale avec ou sans bébé (acrobaties, secrets sur l'oreiller...) : <https://www.eufy.com/eu-fr/blogs/baby/how-to-tell-baby-monitor-hacked>

## Que devrait-on avoir comme modulation ?

Comme dit en introduction, ce type de télécommande est peu cher à réaliser même si parfois elle peut l'être en magasin. Alors la probabilité qu'une modulation de type ASK soit utilisée est très importante. Ce type de modulation est peu coûteuse à planter dans une produit grand publicue... et est parfaitement adaptée à des communications à faible distance.

Il y a 4 grandes familles de modulation numérique dans le domaine des transmissions :

- ASK : Modulation par déplacement d'amplitude - Amplitude Shift Keying
- FSK : Modulation par déplacement de fréquence - Frequency Shift Keying
- PSK : Modulation par déplacement de phase - Phase Shift Keying
- QAM : Modulation d'amplitude en quadrature - Quadrature Amplitude Modulation

Chacune de ces familles comportent des sous familles.

Par exemple, on trouve la BPSK dans la grande famille du PSK. Le « B », c'est pour « Bi », elle est parfois appelée aussi 2-PSK.

Très à la mode depuis quelques années, les radioamateurs ou amateurs de radio utilisent la modulation numérique FSK quand ils communiquent via ordinateurs en FT8 ou JS8, elles sont très similaires :

- FT8 : Franke-Taylor design, c'est une 8-FSK modulation
- JS8 : Jordan Sherer design, c'est aussi une 8-FSK modulation

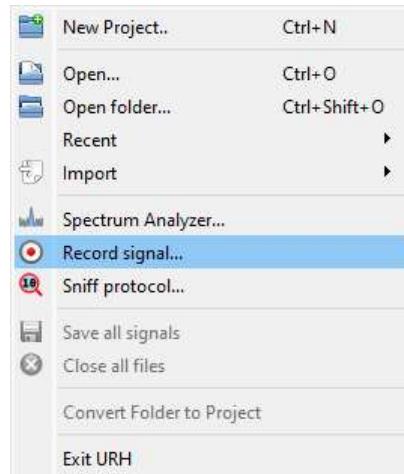
Et là ça semble se compliquer, on a vite fait de dévorer des aspirines car ces noms de modulations, du fait de leurs sous-familles) sont finalement nombreuses et parfois portent plusieurs noms pour un même type de modulation (Voir la base de données Artemis en fin du document).

Ici, je n'aborderai pas les modulations FSK, PSK et QAM car sinon ce ne sera plus un document mais un roman en plusieurs tomes. Je mentionne à la fin du document quelques liens que je trouve digne d'intérêt pour aller plus loin sur ces différents sujets.

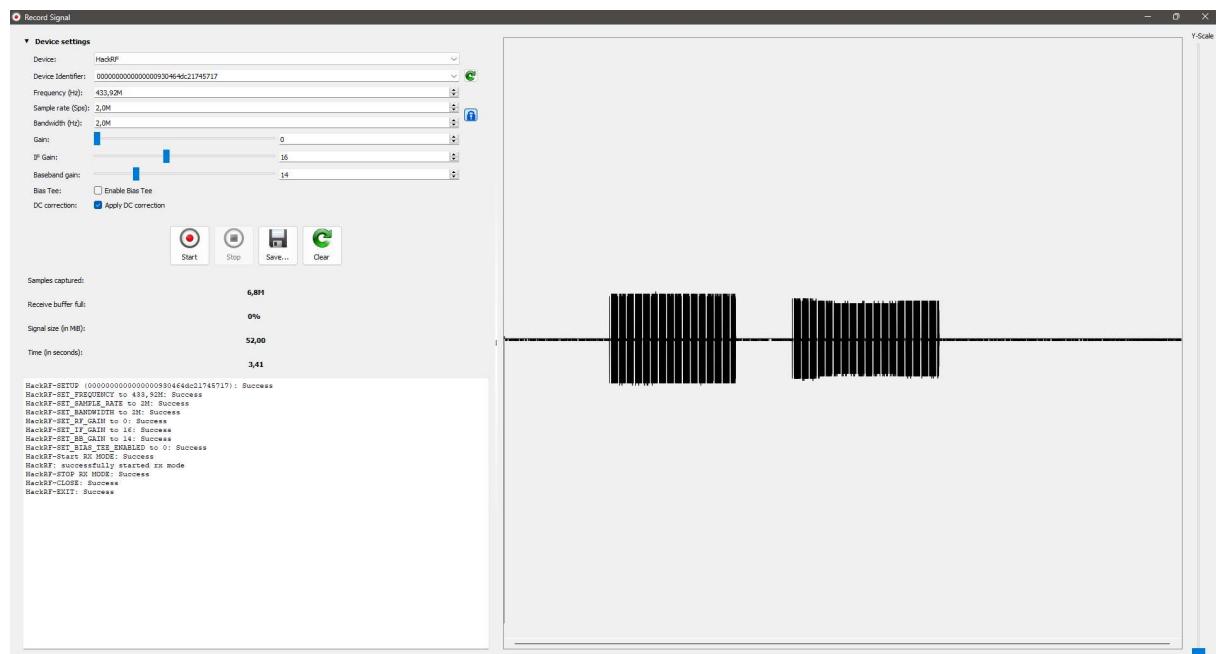
## Universal Radio Hacker : Enregistrer et observer

Maintenant que nous avons validé le fait que nous recevons le signal émis par la clé, nous allons procéder à l'enregistrement de la modulation afin de pouvoir en observer son contenu. Celui-ci contient l'information qui va être nécessaire pour rentrer en communication avec le boîtier de commande.

Direction le menu « File » comme pour l'outil « Spectrum analyser... » mais on sélectionne « Record signal... » :



On obtient la fenêtre suivante. Une pression sur « ON » puis sur « Off » de la clé ou inversement est enregistrée à l'aide des boutons « Start » et « Stop », il reste alors à sauvegarder le fichier avec « Save... ». Si on souhaite renouveler l'enregistrement en effaçant le signal précédent, il suffit de cliquer sur « Clear » et de recommencer l'enregistrement. Les paramètres sont les mêmes que précédemment.

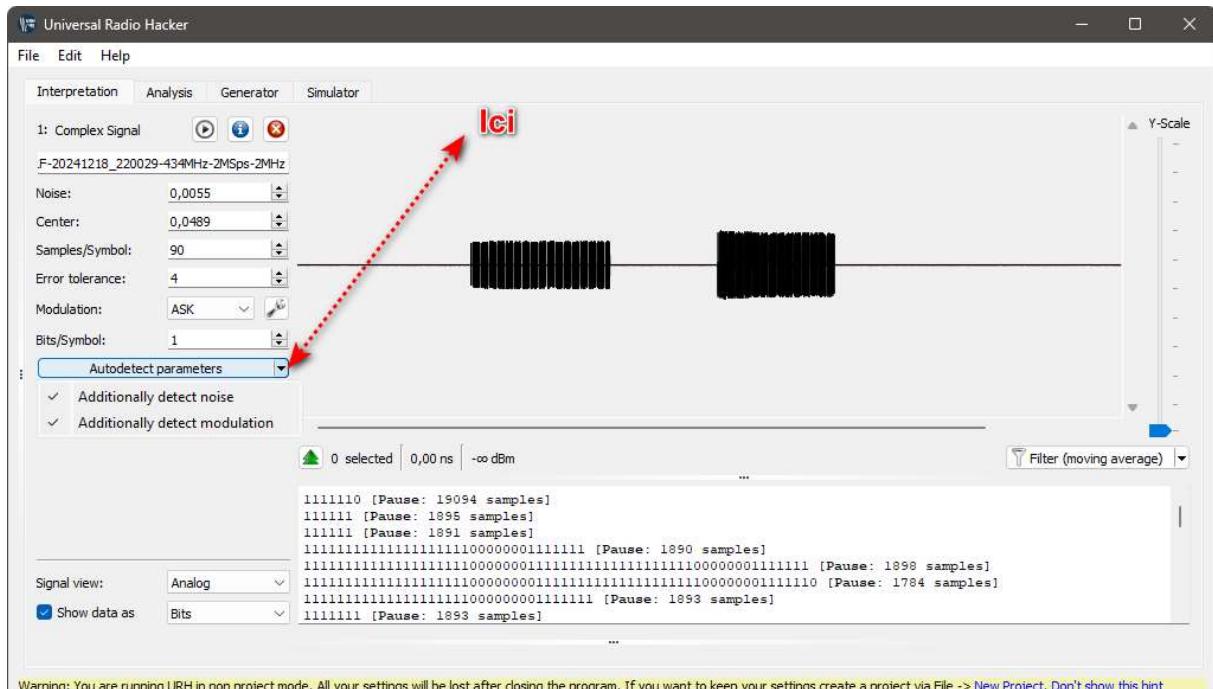


Une fois la fenêtre fermée vous devriez avoir quelque chose qui ressemble à ceci :



Les valeurs de « Noise », « Center », « Sample/symbol », « Error Tolerance », « Bits/Symbol » dans le cadre de ce document n'ont pas besoin d'être modifiés.

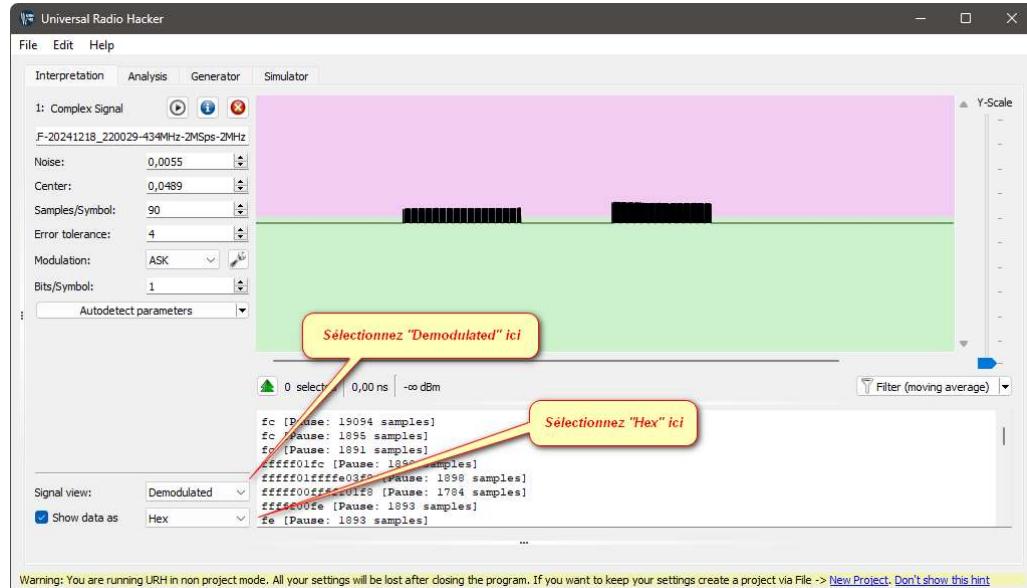
A droite de « Autodetect parameters » il y a comme une flèche qui pointe vers le bas. En cliquant dessus vous aurez accès à un sous menu. Vous y cochez tout en automatique.



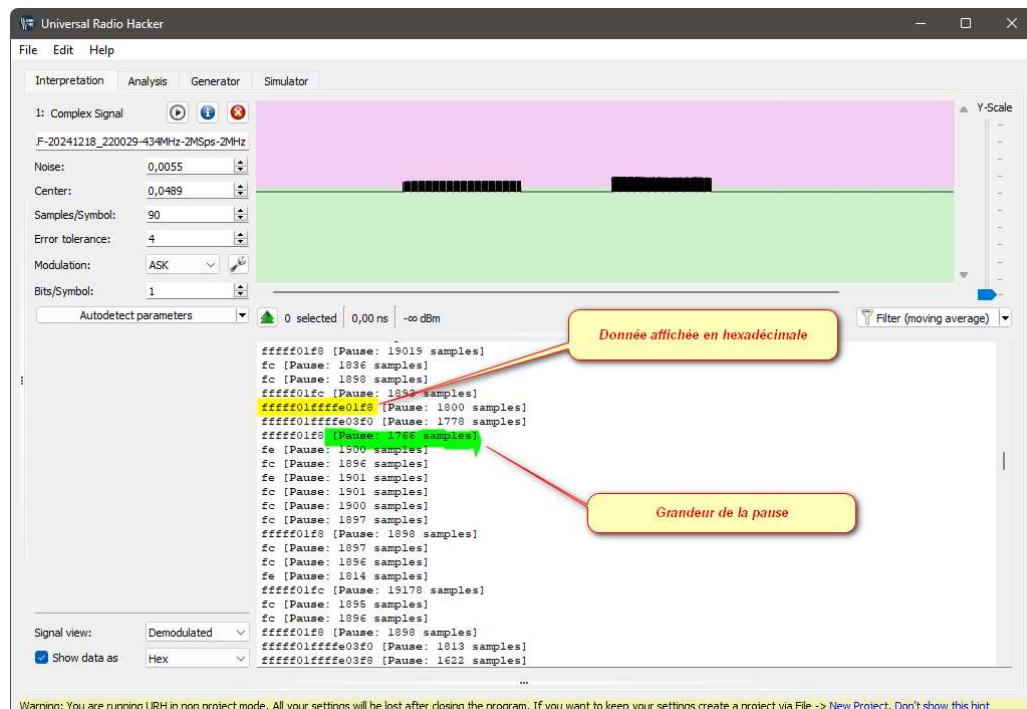
Puis ensuite vous cliquez sur « Autodetect parameters ». Ce qui fait que des paramètres corrects seront appliqués pour démoduler le signal. Ou autrement dit lire contenu de la modulation. Avec un

autre logiciel, si la modulation transportait une voix alors le fait de démoduler permet de la rendre audible.

Je vous suggère de cocher « Show Signal in » et de changer la valeur « Bits » par « Hex » c'est à mon sens plus digeste de lire des données en hexadécimal que de les lire en binaire. Ceci facilite la comparaison des lignes entre-elles.



Nous avons grossièrement 2 rectangles noirs reposant sur une ligne noire avec un fond vert et rose. Tout ceci est précieux et se traduit en lignes qui contiennent une donnée affichée en hexadécimal (Hex) puis il est indiqué des grandeurs correspondant à des pauses.

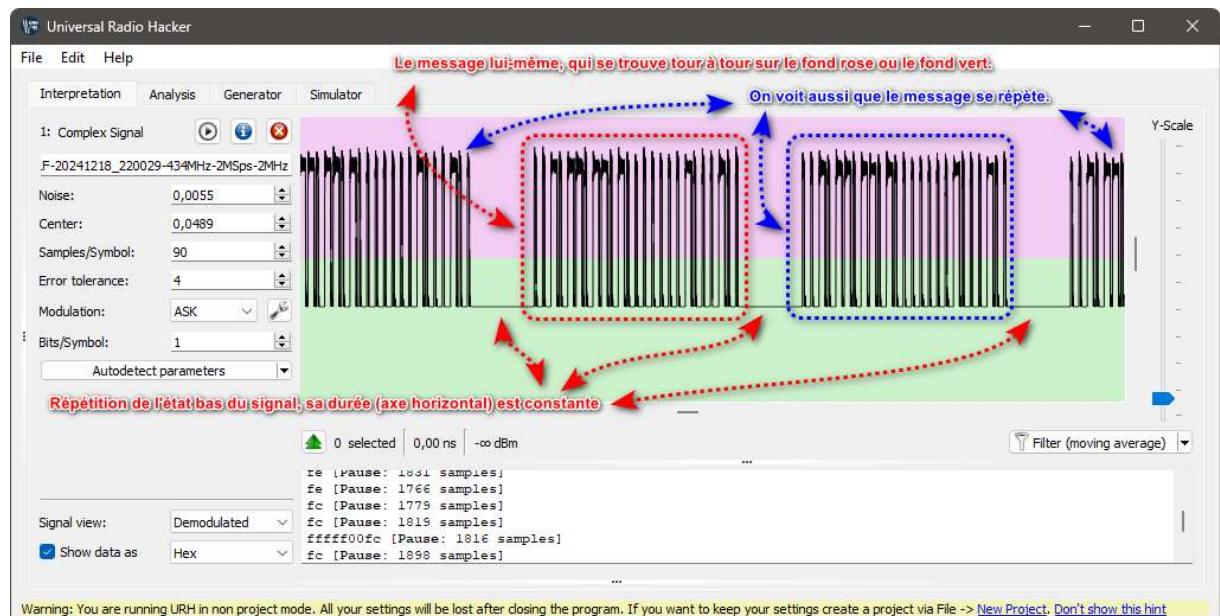


En jouant sur le curseur « Y-Scale », en bas à droite du graphique, il est possible d'agrandir ou de diminuer l'amplitude du signal démodulé. Puis si vous faites rouler la molette sur le dessus de votre souris vous zoomez ou dézoomez dans ce signal. Ce qui vous permet d'obtenir ainsi quelque

chose de ressemblant à ça. En déplaçant le curseur en dessous du signal démodulé vous pouvez alors afficher la partie qui vous convient.



En se promenant dans le signal démodulé avec un niveau de zoom adéquat, on s'aperçoit alors que le la forme du signal se répète.

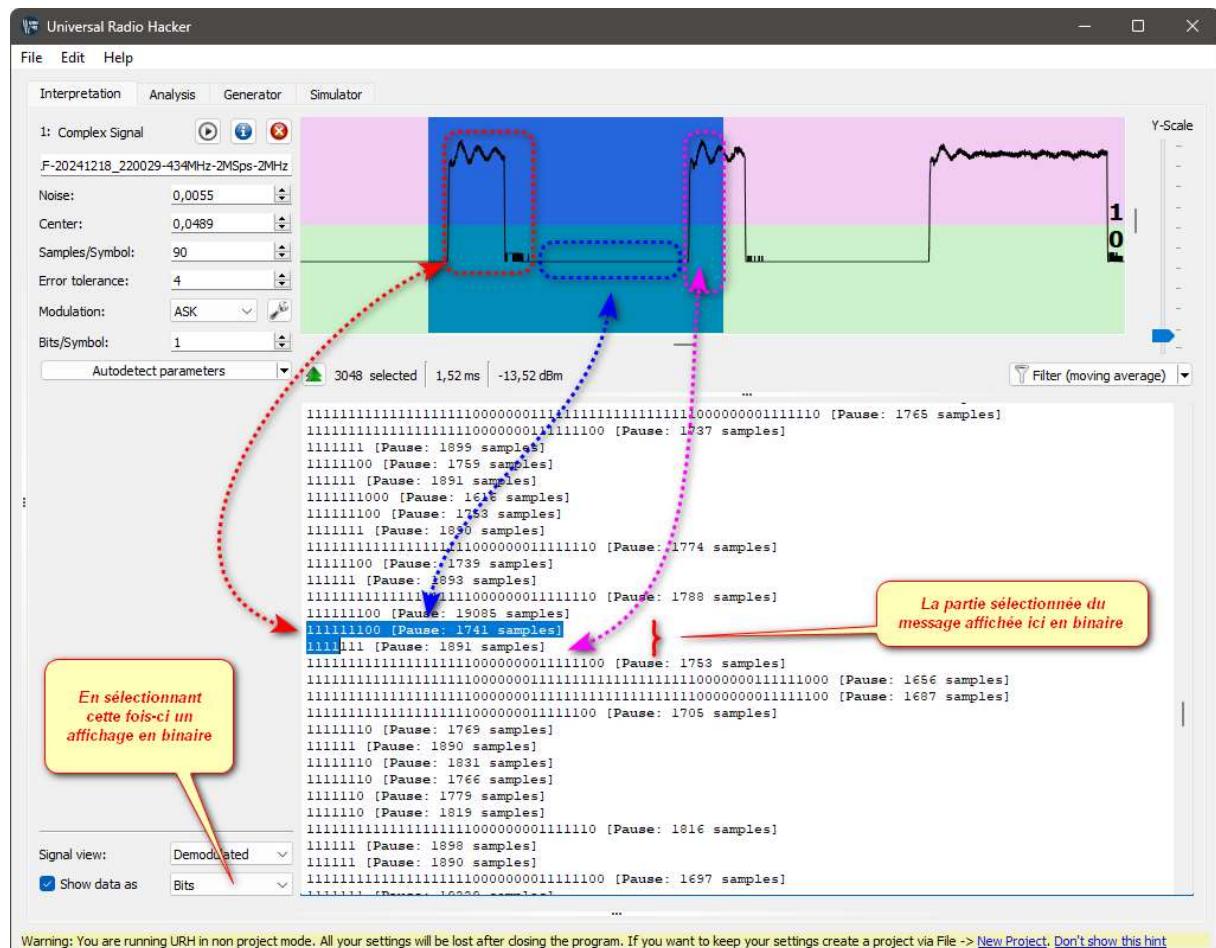


En positionnant le curseur de la souris dans la zone verte ou rose et en réalisant un clic droit alors le menu suivant apparaît et vous sélectionnez « Show symbol legend »



Alors un 1 viendra apparaître dans la partie droite de la zone rose et un 0 dans la partie droite de la zone verte.

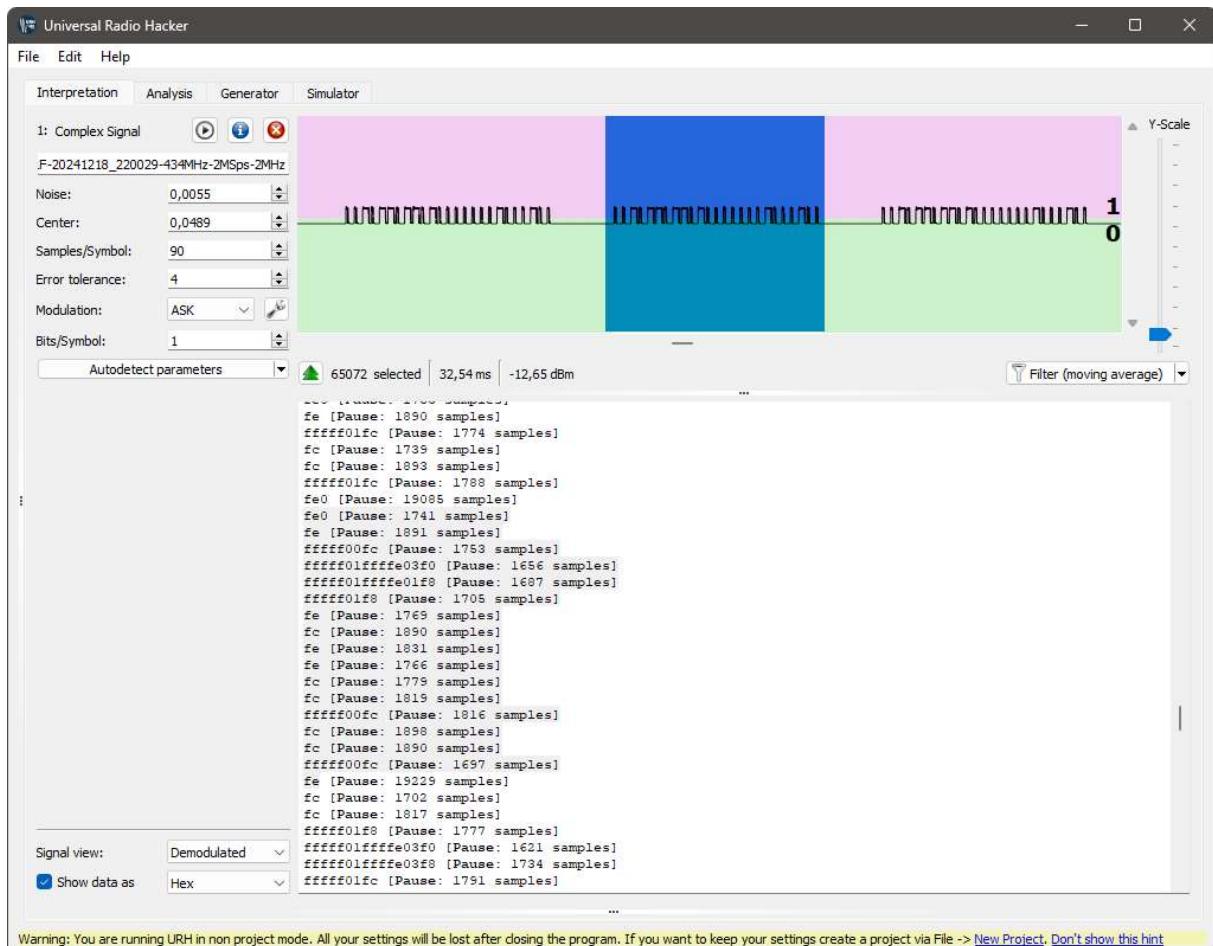
Nous avons un signal numérique envoyé par la clé, il est normal que la donnée numérique alterne entre un niveau 0 et 1 donc tout va bien car nous avons bien à faire à une logique binaire. Si nous choisissons d'afficher l'information en binaire nous pourrions voir ceci et donc vérifier facilement la concordance du graphique avec le message décodé.



Au-delà de rejouer le signal de la clé avec le HackRF pour commander les relais du boitier de commande. Il devient alors tout à fait possible avec cette suite logicielle de dupliquer la clé car nous pouvons afficher le contenu du message. Il est alors aisément de le reproduire avec une autre clé, ou pourquoi pas, par exemple, un Arduino ou autre plateforme à base de microcontrôleur équipé d'un émetteur fonctionnant dans la bande ISM 433.

Une personne indélicate, malveillante qui a accès à votre clé peut alors facilement en faire un double en toute discréption relativement facilement puis la multiplier en autant d'exemplaires qu'elle le souhaite. Ce type de suite logiciel va bien au-delà de rejouer un signal comme peuvent le faire nombre de « plaisantins » avec un outil appelé Flipper Zero ou d'un HackRF équipé du Portapack.

Universal Radio Hacker offre des fonctions de hack qui permettent de réaliser du reverse-engineering, de l'analyse à des fins offensive ou défensive de nombreux systèmes sans fil. L'exemple choisi de la clé est simple car le but de ce document est un coup d'œil initiatique à ce que peut offrir ce genre de solution.



Dans la théorie, le fait d'avoir cliqué sur « Autodetect parameters » a sélectionné les bons paramètres et a positionné « Modulation » sur ASK ».

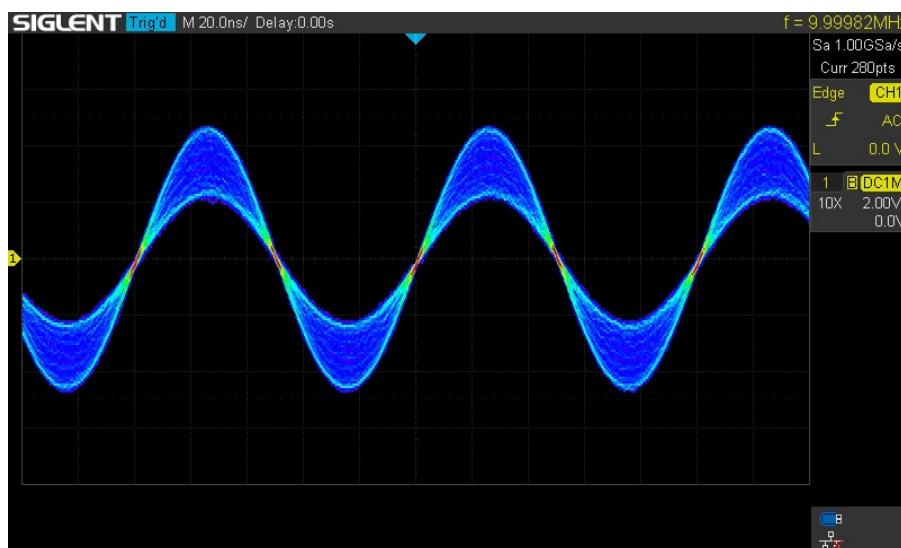
## La modulation

Une modulation contient la donnée transportée, voix, donnée numérique, son, vidéo, image.... Faire l'impasse sur quelques principes de base en serait dommage me semble-t-il. De plus, cela à un rôle prépondérant quand on veut hacker, comprendre, écouter un système radio quel qu'il soit. Pas de panique, les explications données devraient être digestes.

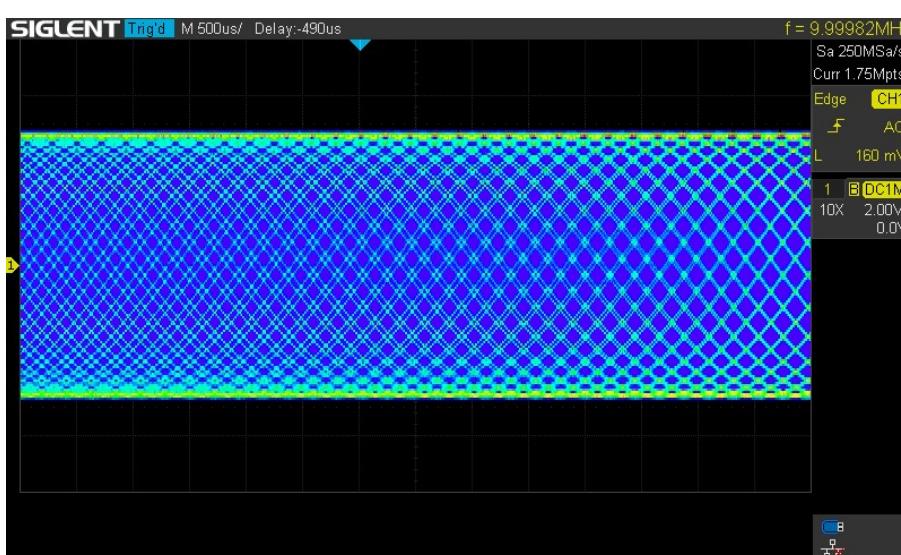
Pour les classiques modulations d'amplitude ou de fréquence utilisées pour transporter un signal comme la voix, celles-ci oscillent autour de la fréquence porteuse.

Dans le graphe ci-dessous, capturé avec un oscilloscope, on voit la modulation évoluer de part et d'autre de la fréquence porteuse.

Ici la fréquence porteuse est de 10 MHz puis le son modulé sur celle-ci est un signal sinusoïdal de fréquence 1 KHz. La modulation évolue dans l'enveloppe bleue sous la forme d'une évolution de l'amplitude d'où son nom Modulation d'Amplitude (AM) :



Concernant la modulation de fréquence (FM), on voit que pour le signal avec la même fréquence porteuse (fréquence d'émission) l'amplitude est fixe mais la fréquence de la modulation évolue.



Le même signal observé avec un analyseur de spectre nous montre qu'effectivement ce signal se répartit de gauche à droite ou inversement sur l'axe de la fréquence porteuse. Donc la fréquence porteuse est au centre de la modulation.

Pour de la FM, là c'est la fréquence de la modulation qui évolue de part et d'autre de la fréquence porteuse.

Si on injecte ce signal à l'entrée d'un analyseur spectre on observe que la modulation dans les deux cas se positionne également autour de la fréquence centrale qui est alors la fréquence porteuse.

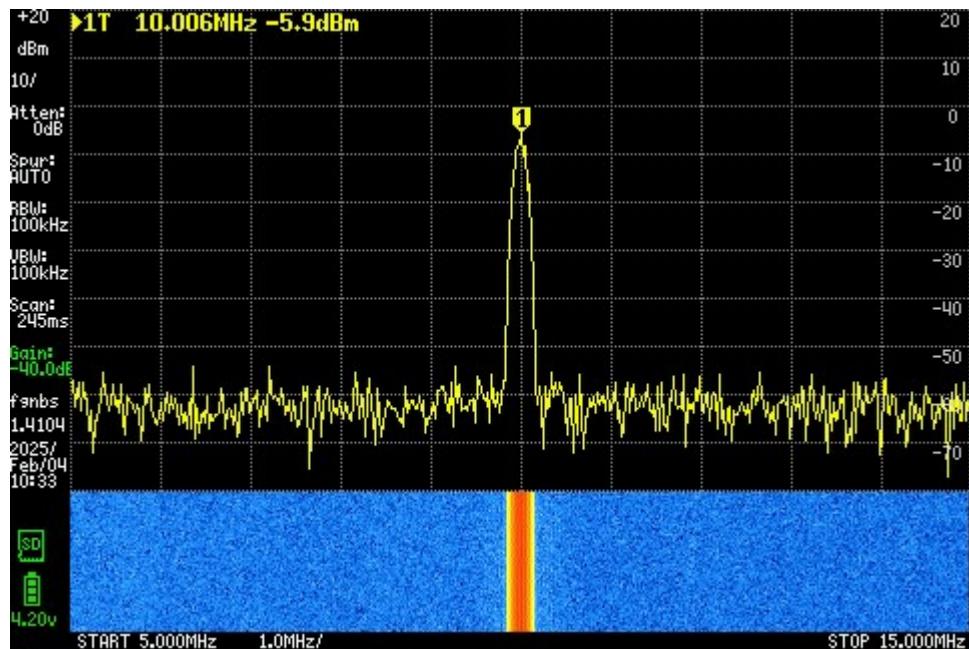


Figure 2: Modulation d'Amplitude (sinusoïde à 1KHz) sur une fréquence porteuse de 10 MHz

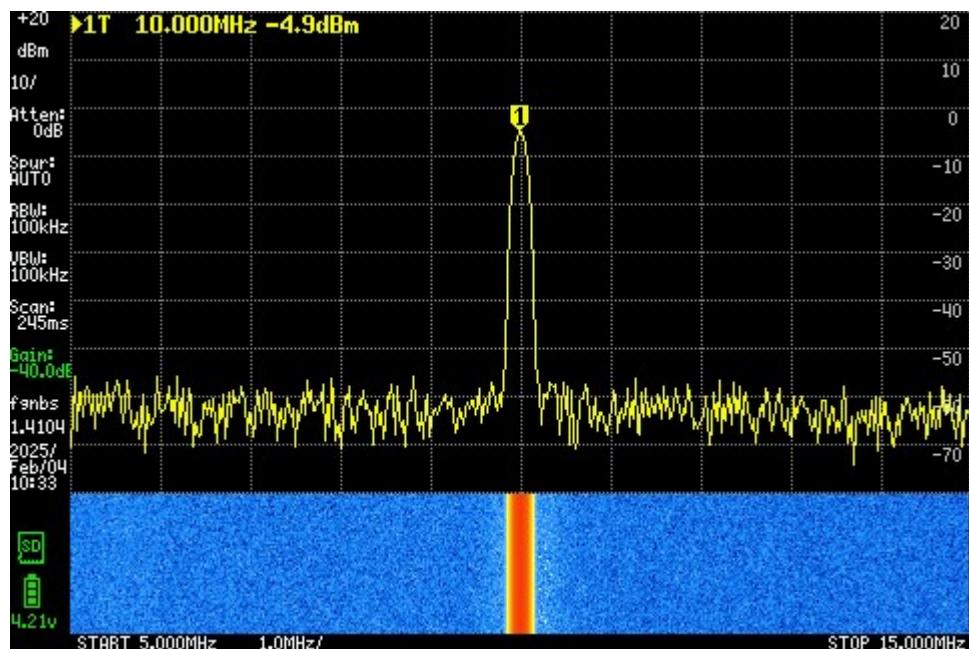


Figure 3 : Modulation de Fréquence (sinusoïde à 1KHz) sur une fréquence porteuse de 10 MHz

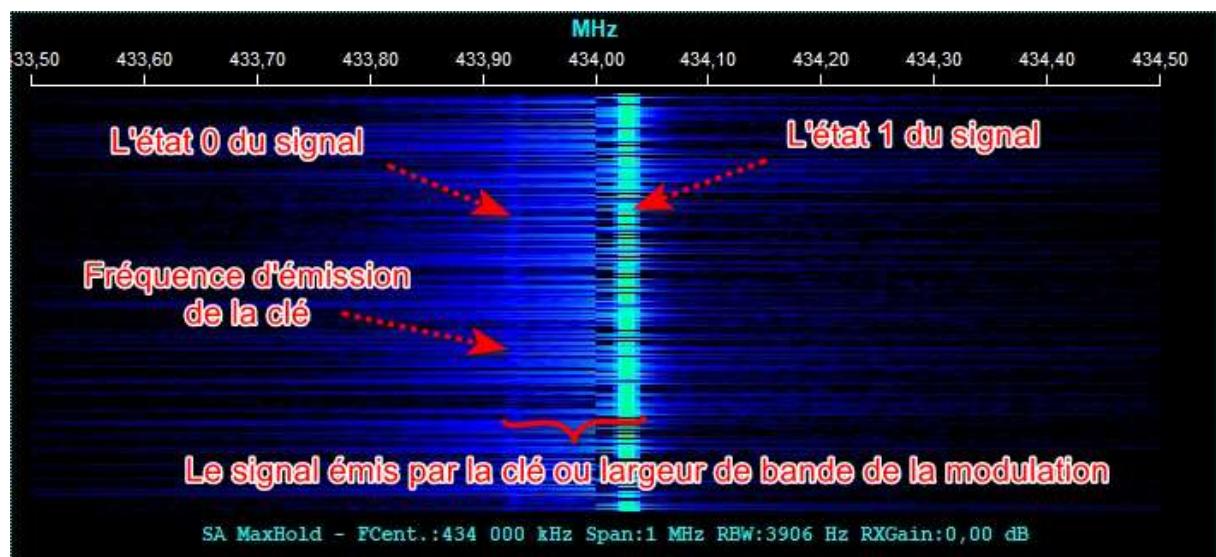
Concernant les modulations transportant des signaux numériques, on ne peut plus considérer par défaut que la fréquence porteuse est centrée par rapport à la modulation. Donc le pic d'énergie qui

apparaît sur le graphe de l'analyseur de spectre correspond à autre chose que la fréquence porteuse ou aussi appelée la fréquence d'émission. Pour autant celle-ci n'est jamais très loin 😊

Dans le cas du signal modulé de notre clé, si on observe le waterfall (chute d'eau), ce graphe plein de couleurs, on voit nettement que c'est différent. Nous avons à faire à une modulation numérique. Il y a donc les 0 et les 1 qui vont se traduire visuellement sur le graphe. La modulation ASK et plus particulièrement sa sous famille la modulation OOK à la particularité de ne pas émettre d'énergie pour l'état 0 et de transmettre son maximum d'énergie lorsqu'il y a un état 1 à transmettre.

En observant le waterfall ci-dessous, on voit qu'il y a 2 droites parallèles et verticales. L'une est particulièrement visible en bleu « pétard » et l'autre se confond presque avec le bruit et se trouve à sa droite.

Dans le cadre de la modulation OOK, l'état 0 correspond à la fréquence porteuse donc ici 433,92 MHz et l'état 1 a environ 434 MHz. Si on fait la différence de ces 2 fréquences on identifie alors la bande passante de la modulation, soit 80 KHz.



Afin d'aborder simplement les choses, on peut considérer qu'un signal radio peut être comparé à un véhicule avec un passager. Alors nous avons :

- Le véhicule est la fréquence porteuse soit la fréquence d'émission de l'émetteur. Donc ici notre émetteur (la clé) émet (en Europe) sur la fréquence de 433.92 MHz.
- Le passager devient alors la donnée transportée par le véhicule. Ce passager est notre modulation. Et là, son type, n'est pas nécessairement indiqué sur la notice où à l'arrière du produit. Il va falloir peut-être jouer aux devinettes. Tant qu'on n'aura pas identifié le type de modulation on ne pourra pas procéder à l'extraction de la donnée contenue.

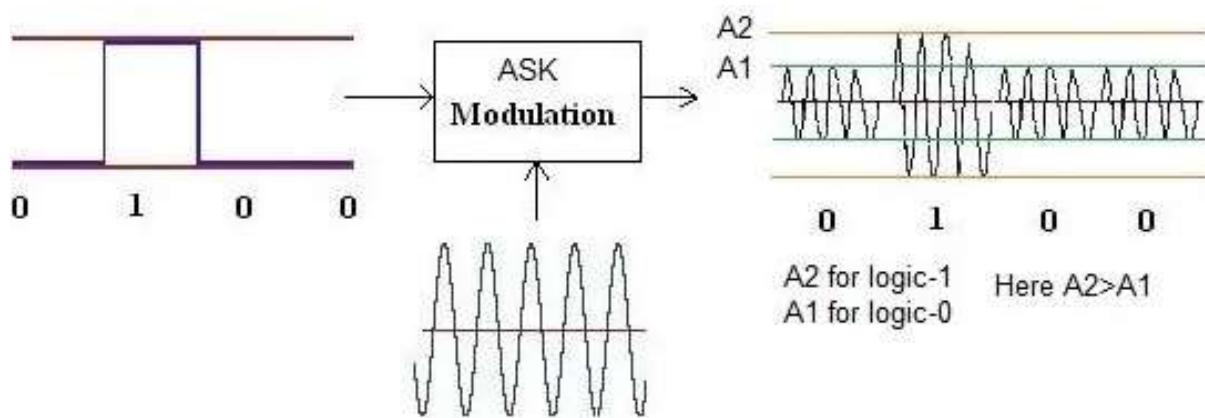
Un peu plus haut j'ai mentionné le fait qu'il y a 4 grandes familles de modulation numérique. Je vais m'arrêter ici sur les 3 premières : ASK, FSK et le PSK. Ces modulations ont des formes caractéristiques permettant de les reconnaître facilement une fois qu'on a compris le sens de la première lettre de leur acronyme.

## La modulation ASK

La modulation ASK (Amplitude Shift Keying) c'est d'une certaine manière l'AM utilisée par les cibistes, radioamateurs... En effet selon l'état du signal numérique à véhiculer, l'amplitude du signal modulé va évoluer.

En mode "shift keying", lorsqu'un "1" apparaît, l'amplitude du signal passe en A2 et lorsqu'un "0" apparaît l'amplitude du signal passe en A1. La modulation par déplacement d'amplitude (ASK) est équivalente à la modulation d'amplitude dans un signal analogique (voix par exemple), sauf qu'il s'agit d'un nombre binaire multiplié par le signal de fréquence porteuse. Le décalage d'amplitude utilise la fréquence et la phase comme constantes, l'amplitude comme variable et les bits d'information sont transmis via l'amplitude de l'onde porteuse.

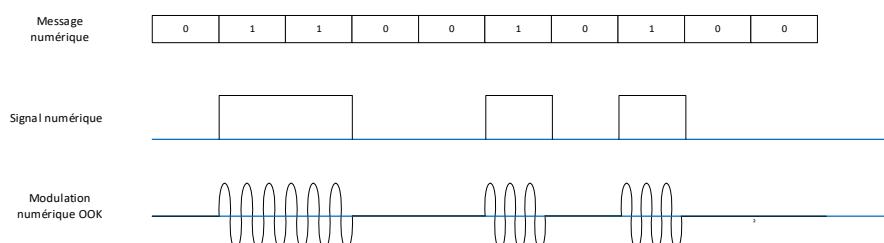
Il se passe alors ceci :



## La modulation OOK

Cette modulation est une forme dérivée de l'ASK. Elle est utilisée par la clé. Comme elle fait partie de la famille ASK, URH ne le précise pas. Si vous entamez la lecture du chapitre suivant, vous verrez alors que le contenu de certains liens présentés parlent de modulation OOK au sujet de ce type de clé. Mais qu'est cette particularité de OOK parfois appelée 2ASK ou modulation binaire d'amplitude :

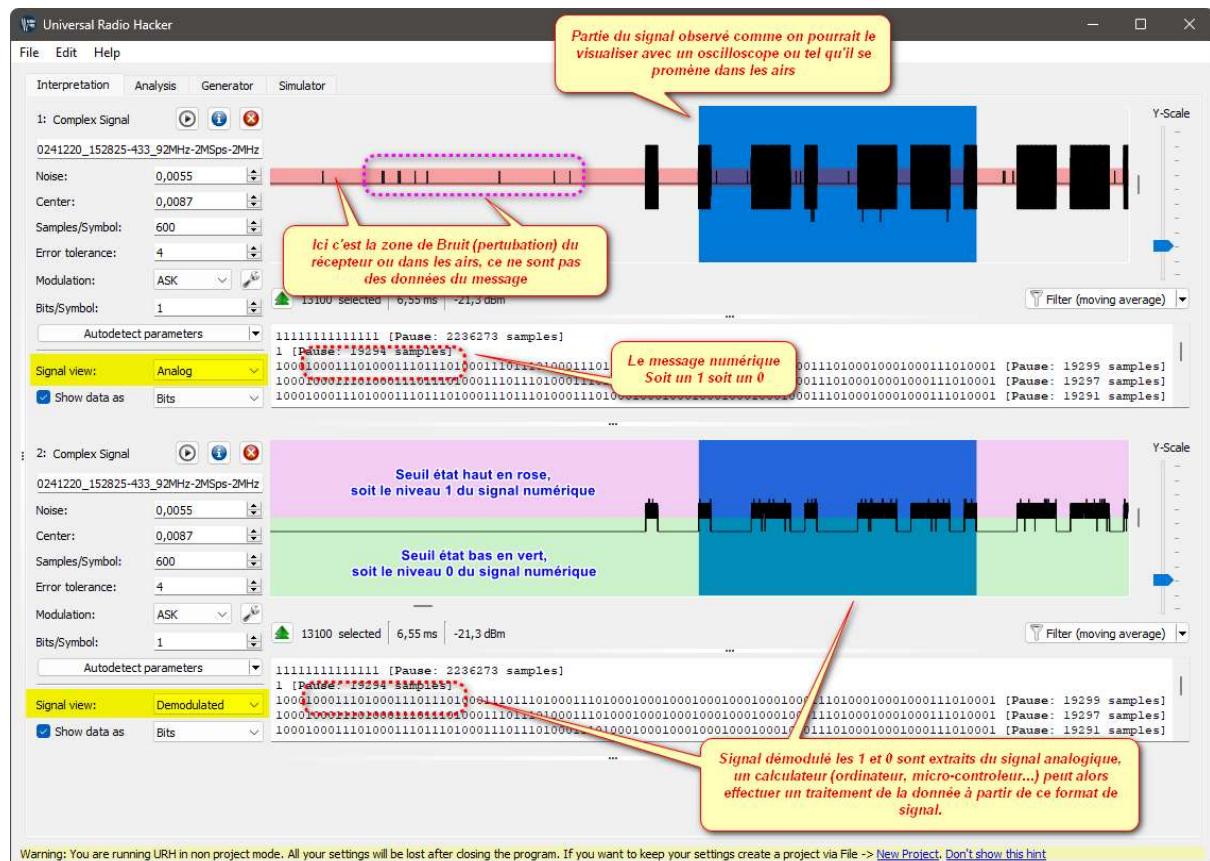
- On peut traduire littéralement que la modulation OOK (On Off Keying) est un signal binaire dont l'état bas (0) s'évanouit sur son abscisse et dont l'état haut (1) transporte un signal dont la longueur varie en fonction du nombre de bit à l'état 1.
- La modulation OOK est la plus économique en énergie car elle consomme la totalité de l'énergie nécessaire que lorsqu'un « 1 » est envoyé.
- Graphiquement cela nous donne ceci :



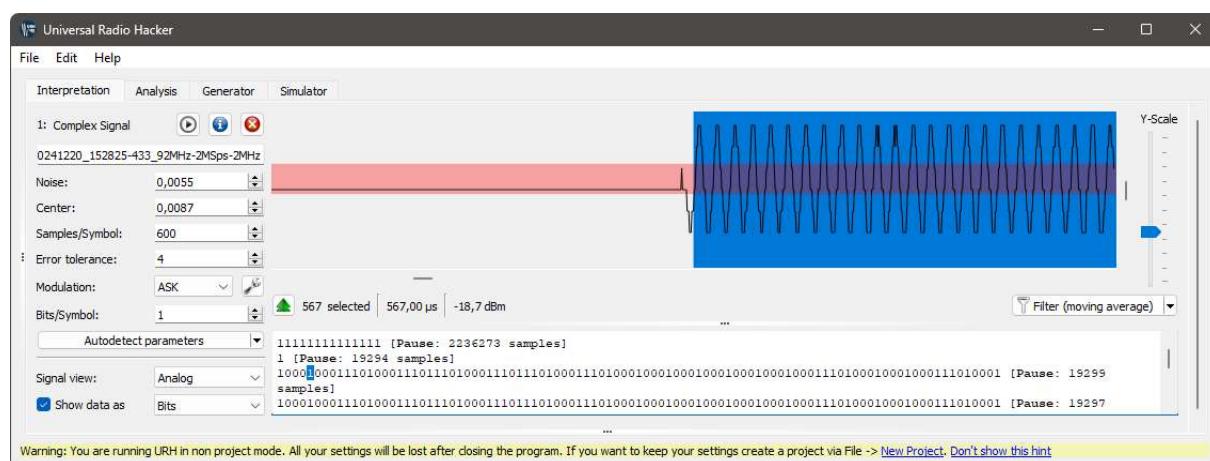
Pour les radioamateurs, amateurs de radio, les lecteurs de Picsou Magasine, les scouts.... On peut tout à fait faire une analogie avec un signal que vous connaissez tous, c'est le Morse ou aussi appelé

CW pour les intimes. Il y a beaucoup de discussions à ce sujet afin de savoir s'il s'agit d'une communication numérique binaire, ternaire, quaternaire..., certains citent même Shannon pour argumenter leur discours mais Shannon n'est plus là pour affirmer ou infirmer ce qu'il en pense. Le seul consensus c'est que la CW est une modulation numérique, ouf !

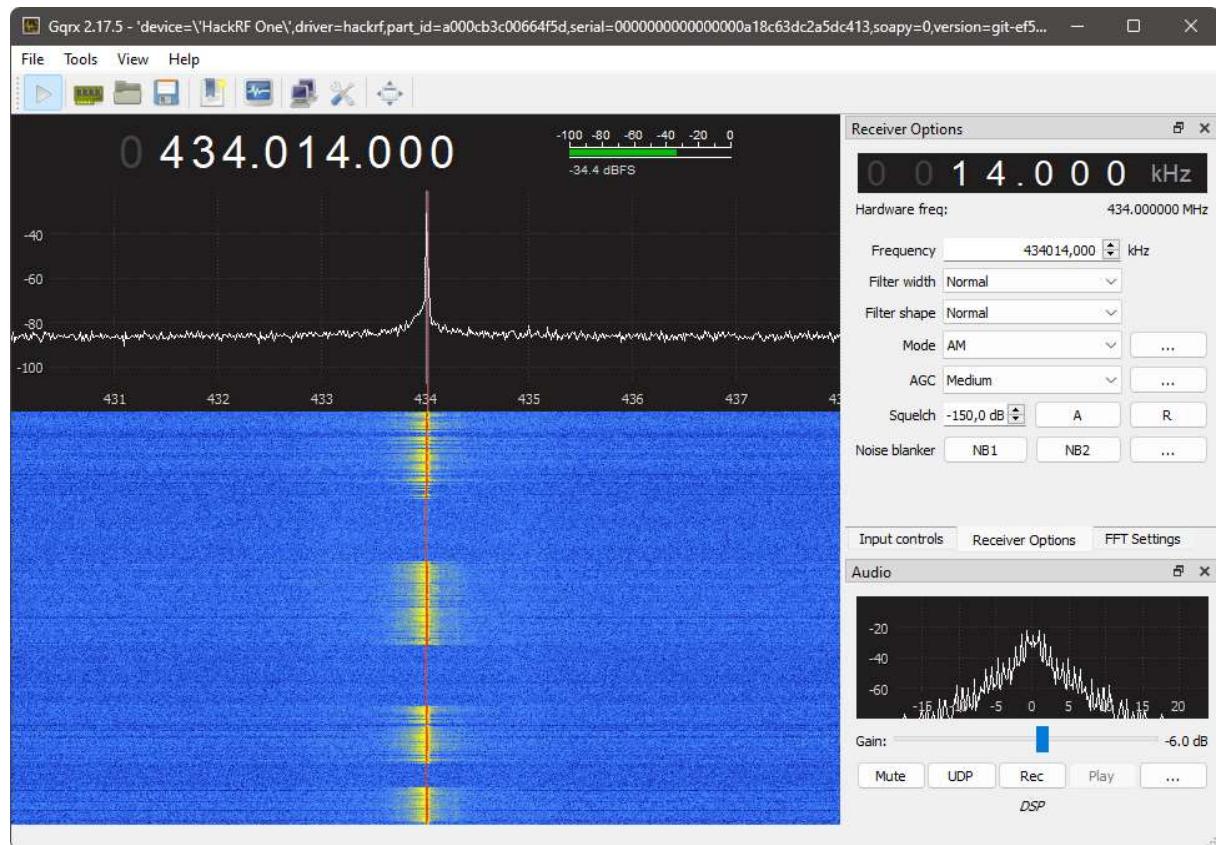
Voici un même signal émis par la clé et reçu par le HackRF puis traité par URH. Il est présenté, en haut, non démodulé (brut) et démodulé (en bas). On peut voir qu'on a à faire effectivement à une modulation OOK appartenant à la famille des modulations de type ASK. En effet à l'état bas (0) de la donnée numérique le signal RF est à 0 et uniquement quand il y a un état haut (1) on voit apparaître la modulation.



Avec ici un zoom sur uniquement un seul bit du message :



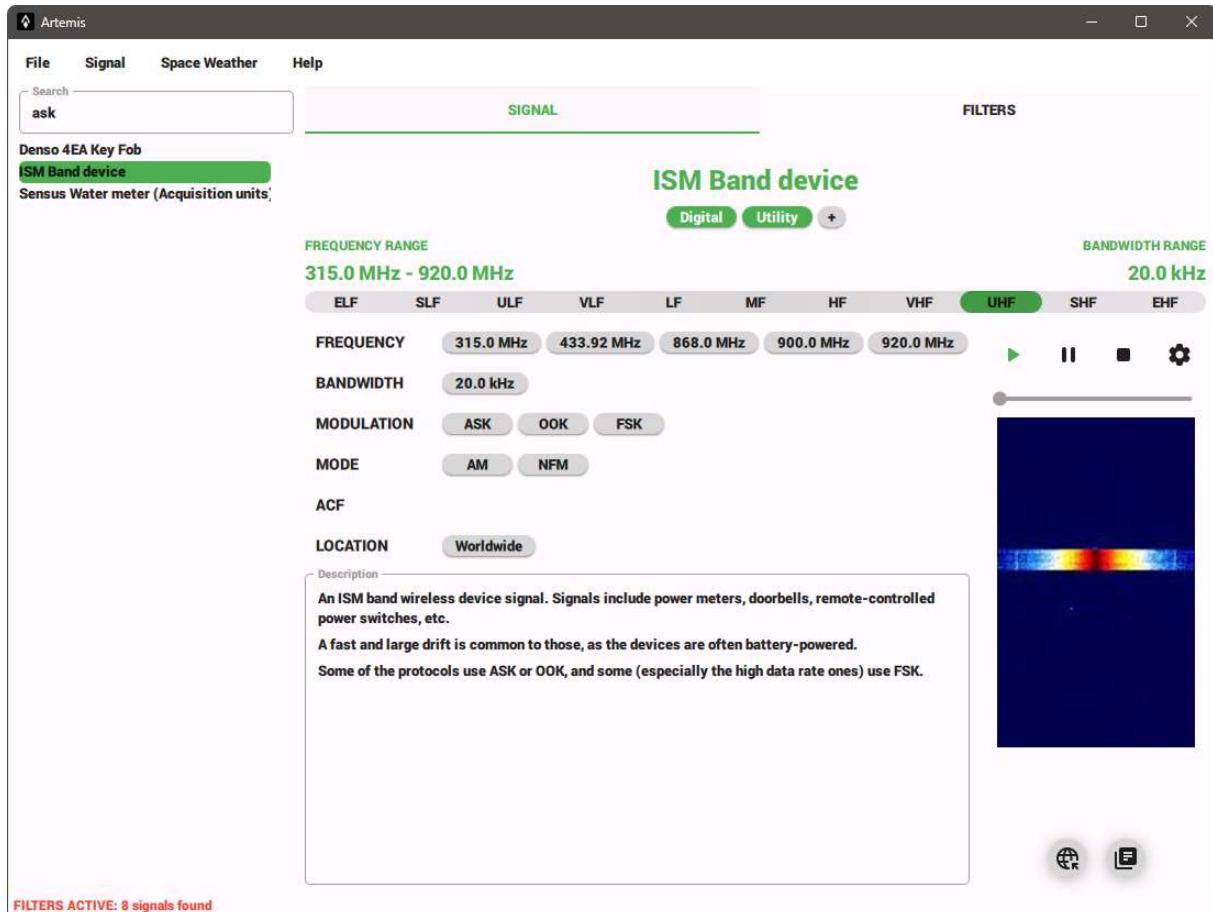
En utilisant un logiciel SDR comme Radio-Console, SDR # ou d'autres comme GQRX, si vous écoutez le signal émis par la clé vous aurez une idée des sons produits et cela pourra vous faciliter la vie en réalisant des écoutes sur d'autres bandes ISM par la suite ou même sur celle-ci. Former son audition à ces différents sons idem pour l'image du Waterfall (chute d'eau du SDR) est important, il me semble si on souhaite s'investir dans cette activité d'analyse des signaux RF numérique. Le logiciel Artemis est d'ailleurs d'une grande aide pour cela :



J'utilise GPRX sous Windows 11 grâce à la suite logicielle Radioconda (voir le lien à la fin du document dans le chapitre : « Cybersécurité et communication sans fil »).

Le spectre audio en bas à droite de la copie d'écran ci-dessus montre très nettement la forme caractéristique de la modulation OOK.

Voici une copie d'écran d'Artemis au sujet des équipements émettant sur les bandes ISM. Les deux éléments d'identification que sont l'audio du signal et sa forme sur le waterfall y sont présents. Ce qui peut aider à confirmer ou pas une présomption de modulation.



Si vous aimez les aspirines ou que vous n'en avez pas besoin pour lire le langage des mathématiques alors voici un document décrivant ces 4 grandes familles de modulations et aussi la modulation OOK. Il est rédigé dans cette langue très utilisée dans les matières scientifiques (anglais) :

[http://physique.elec.free.fr/Annee\\_2/Ch5\\_Modulations\\_numeriques.pdf](http://physique.elec.free.fr/Annee_2/Ch5_Modulations_numeriques.pdf)

## Emettre un signal

Le fait d'utiliser un HackRF va permettre d'émettre un signal de commande en direction du boîtier. Le claquement du relais va alors valider que celui-ci l'a bien reçu puis interprété.

Recevoir et interpréter sont deux choses différentes. En effet, je rappels que le boîtier de commande doit reconnaître la clé à l'aide de son identifiant puis obtenir la commande appropriée. Commande qui entraîne le mouvement des contacts du relais. Ces informations étant dans le message contenu dans la modulation OOK.

Pour émettre, il faudra donc vérifier l'exactitude des points suivants pour que le boîtier de commande réagisse correctement :

- Fréquence d'émission : 433.92 MHz
- Modulation : ici de l'ASK car le OOK appartient à cette famille de modulation. Un mauvais choix de modulation et le boîtier ne sera pas en mesure de démoduler le message transmis même s'il reçoit bien le signal RF.
- Identifiant de la clé
- La donnée de commande

## Emettre, des précautions pour éviter la casse

Emettre nécessite d'avoir une antenne adaptée en impédance à la sortie de l'émetteur. Ceci est indispensable si on souhaite garantir la survie de son émetteur dans le temps (même très court).

L'immense majorité des émetteurs, aujourd'hui, ont une impédance ( $Z$ ) de sortie de 50 Ohms. Si la charge (antenne, amplificateur RF, filtre...) qui se trouve connectée à sa sortie ne respecte pas cette impédance dans une certaine proportion, l'étage de sortie de votre émetteur va très probablement « griller ».

D'où l'importance de vérifier le SWR en sortie de votre émetteur quand celui-ci passe à l'émission sur sa charge. L'équipement le plus répandu pour effectuer cette vérification est le Tosmètre voir aussi Rosmètre ou appelé en anglais SWR meter. La sortie d'un émetteur est conçue pour supporter sans dommage un SWR allant jusqu'à 2.

Plus le SWR, en sortie d'émetteur, va être important moins il y aura de puissance RF qui va être rayonnée par l'antenne. Cette puissance qui n'est pas rayonnée par l'antenne est appelée alors puissance réfléchie.

Plus cette puissance réfléchie sera importante plus le SWR va grimper et plus l'émetteur a le risque de voir, au moins, son étage final de griller.

Voici quelques grandeurs :

- SWR 2 => 10 % de puissance réfléchie. L'antenne rayonne 90 % de la puissance.
- SWR 1.5 => 4 % de puissance réfléchie. L'antenne rayonne 96 % de la puissance.
- SWR 1.2 => 0.8 % de puissance réfléchie. L'antenne rayonne 99.2 % soit quasiment la totalité de la puissance du signal émis par l'émetteur.

Un SWR de 3 donne une puissance de réfléchie de 25% ce qui commence à devenir compliqué pour l'étage final de l'émetteur à gérer en termes de dissipation thermique. Surtout si le gain d'amplification est au maximum de l'étage final. Un SWR > 3 est rapidement fatale si on insiste. Un exemple : Si la puissance maximale de votre émetteur est de 100W et que votre gain d'amplification

est réglé à son maximum, on aura alors 25W de puissance réfléchie à faire dissiper par l'étage de sortie de l'émetteur, ce qui commence à faire beaucoup pour celui-ci, il risque donc de griller rapidement.

Voici une table, au format PDF, de chez Marki (grand industriel de la RF) qui met en perspective SWR (VSWR), puissance réfléchie (Reflected Power), puissance disponible pour la charge ou l'antenne (Through Power) et d'autres informations utiles : <https://markimicrowave.com/tools/return-loss-to-vswr.pdf>

Un SWR de 2 est généralement admis comme sans risque pour l'étage final d'amplification de l'émetteur. Il est normalement conçu pour absorber environ 10 % d'énergie correspondante (puissance réfléchie).

J'ai conscience que la plupart d'entre nous ne possède pas de SWR meter adapté à cette gamme de fréquences (attention un Tosmètre dit de cibi n'est pas adapté, sa plage de fréquences n'est pas adaptée).

Si vous possédez un NanoVNA, vous pouvez vérifier le SWR de l'antenne assez facilement. Cet équipement est un Vector Network Analyser (VNA) simplifié mais qui pour autant s'avère très utile dans le domaine des radiofréquences. J'ai publié plusieurs articles à son sujet dans mon blog si vous souhaitez le découvrir. Son usage ne se limite pas aux antennes et à la mesure de SWR. De plus, il vous permettra de vérifier aussi le câble coaxial reliant votre émetteur à votre antenne si c'est le cas (mesure d'impédance, mesure de longueur...).

Pour échapper à cette mesure et limiter le risque de griller l'étage de sortie du HackRF, il est possible de prendre des précautions ou plutôt de se fixer une limite avant de passer à l'émission.

Cette limite consiste à réduire le gain d'amplification de l'émetteur. En plaçant à proximité le boîtier de commande du HackRF, sa puissance minimum d'émission sera largement suffisante pour commander le boîtier. Du coup, l'étage de sortie du HackRF sera en mesure d'encaisser la puissance réfléchie du fait de l'adaptation en impédance non adéquate.

**Ne jamais, jamais... mais jamais émettre sans antenne.** Toute la puissance sera réfléchie dans l'étage de sortie. L'énergie ne pourra pas se dissiper et la montée en température sera probablement rapide et fatidique pour le HackRF One.

Si vous souhaitez tester certaines fonctionnalités de la suite logicielle Universal Radio Hacker sans pour autant avoir besoin de rayonner en émission au-delà du mètre. Une solution consiste à utiliser une charge fictive de 50 Ohms (impédance de sortie de l'émetteur). C'est une chose qui peut se réaliser facilement avec une résistance au carbone de  $\frac{1}{4}$  watts. L'étage de sortie du HackRF sera heureux car sa puissance se dissipera dans la résistance avec une impédance de charge adaptée. Dans la théorie une charge fictive ne rayonne pas mais pour autant la réalité est différente. Donc en l'absence d'antenne adaptée ce peut être une solution pour protéger le le HackRF.

Si vous réalisez cette solution, attention de bien utiliser une résistance au carbone et non une à couche métallique, bobinée.... Une résistance au carbone de 47 Ohms fera parfaitement l'affaire pour obtenir un SWR < 2 et probablement très proche de 1 si vous avez câblé proprement ce montage.

## Réaliser une charge fictive

Pour le HackRF, une charge fictive est une simple résistance au carbone d'environ 50 ohms. La dimension (encombrement) d'une charge fictive varie en fonction de la puissance qu'elle est en mesure d'absorber. Là une résistance de 47 ohms au carbone 1/4 watt est largement suffisante. La puissance d'émission du HackRF One a un maximum de +15 dBm selon son concepteur, ce qui donne une puissance maximale de 32 mW. Une résistance 1/4W est capable de dissiper 250 mW. Le code couleur de la résistance étant : Jaune Violet Noir



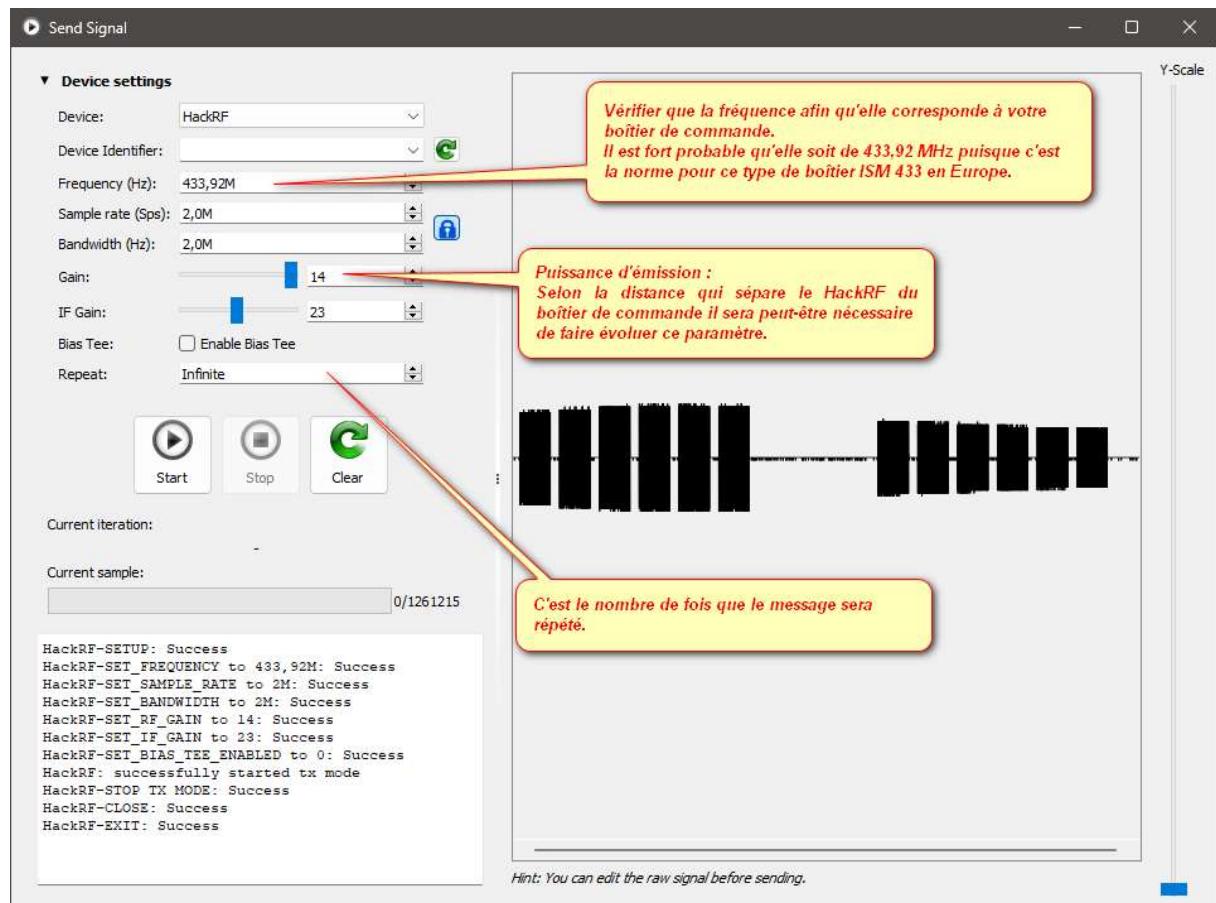
Figure 4: Les pattes de la résistance sont coupées au plus court et tout particulièrement sur le côté soudé à l'âme du connecteur !

L'idéal est de placer ce montage dans un boîtier métallique avec une connexion à la masse réalisée (boîtier à la masse du connecteur). Au moment de la réalisation du montage, il est important que les pattes de la résistance soient coupées au plus court surtout sur la patte qui est soudée à l'âme du connecteur.

Si vous avez un nanoVNA alors vous pouvez entre autres vérifier sa plage de fréquences où le SWR sera inférieur à 2.

## Emettre le signal enregistrer

Comme nous venons de le voir, émettre sans connaître l'impédance de la charge (antenne) c'est prendre un risque de griller l'étage de sortie RF de l'émetteur. Pour éviter tout désagrément si vous utilisez une antenne inconnue (bande passante, impédance) le plus simple est de diminuer la valeur du gain de l'amplificateur RF à son minimum. C'est le premier paramètre de la fenêtre suivante qu'il est préférable de régler (Puissance d'émission).



Dans la fenêtre « Send Signal » on retrouve le bouton « Start » qui va permettre d'envoyer le signal. Pour stopper l'émission le bouton « Stop » devrait être efficace 😊

La fonction « Repeat » peut avoir du sens, car en position « Infinite » l'émission perdurera avec le risque de griller l'étage de sortie RF du HackRF si l'antenne n'est pas adaptée à celui-ci.

J'avoue, comme beaucoup, j'utilise une simple antenne télescopique pour les expériences de ce type, il est évident qu'elle a peu de chance d'être adaptée en impédance à la sortie antenne du HackRF, pour éviter les problèmes liés à SWR>2 j'évite de répéter indéfiniment le message émis. Puis en baissant la valeur du gain à son minimum c'est encore mieux si le boîtier est à proximité.

Sur la copie d'écran, on voit l'amplitude du signal augmenter et diminuer. Ceci vient juste du fait que j'ai rapproché la clé du HackRF au moment de capturer le signal, puis je l'ai éloigné au moment de stopper la capture.

Après avoir cliqué sur « Start » le HackRF va émettre le signal et normalement le relais va changer d'état. Ce qui va se traduire par un claquement qui devrait être audible. Attention, votre télécommande possède probablement 2 boutons. Si vous émettez 2 fois de suite la même commande, il est normal que le relais de « claque » pas.

Donc au préalable, il est nécessaire d'enregistrer le signal correspondant à chaque bouton. Deux possibilités alors apparaissent :

- Sois-vous réalisez un seul enregistrement où vous alternez les pressions sur les boutons de la clé.
- Sois-vous enregistrez autant de signaux que de boutons et vous les jouez tour à tour.

Personnellement je préfère la seconde option ce qui facilite la comparaison des signaux lors de l'analyse.

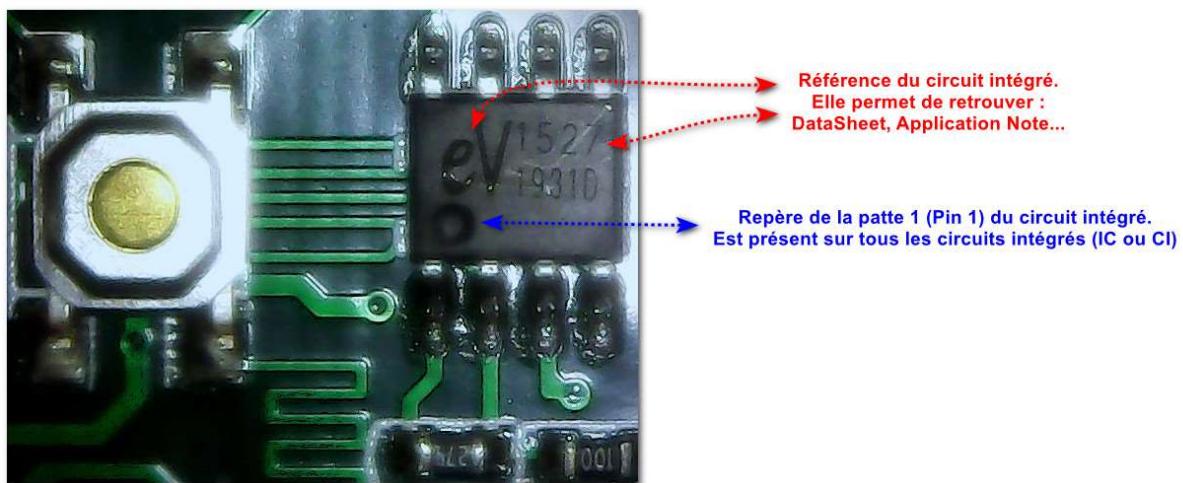
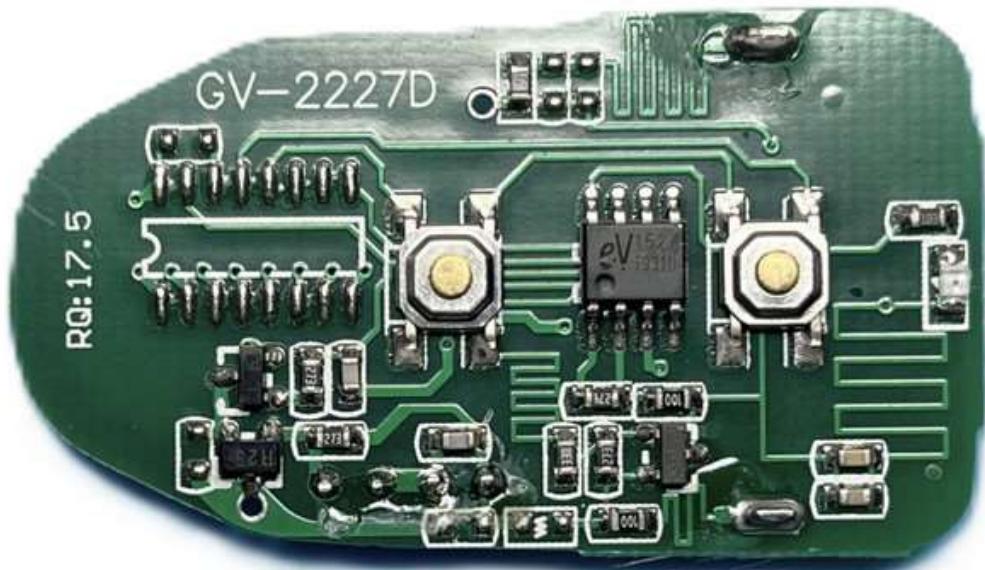
## Autopsie de la clé

Une carte électronique contient un certain nombre de composants électroniques. Pour les plus complexes comme les circuits intégrés, il est tout à fait possible de s'appuyer sur deux types de documents afin d'en comprendre leur rôle. C'est-à-dire :

- DataSheet (Fiche technique du document)
- Application Note (ce document n'est pas systématiquement présent, mais il peut exister et donne des exemples d'usages plus ou moins commentés)

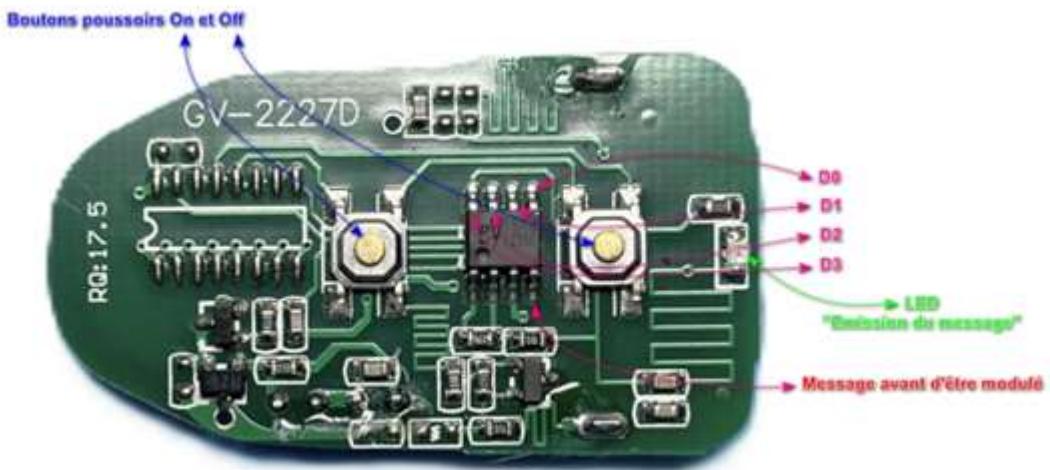
Comme le montre la photo de la clé ci-dessous, il n'y a qu'un seul circuit intégré ici. Il génère le message contenu dans la modulation ASK.

Il est bon de prendre en compte le fait qu'un même composant peut avoir des équivalences ou livré sous différentes formes de boîtiers.



Avec la fonction « Analyseur Logique » d'un oscilloscope ou un analyseur logique (plus performant) on peut tout à fait lire le contenu du message quand on enfonce On et Off pour le comparer au résultat de l'analyse obtenue avec URH.

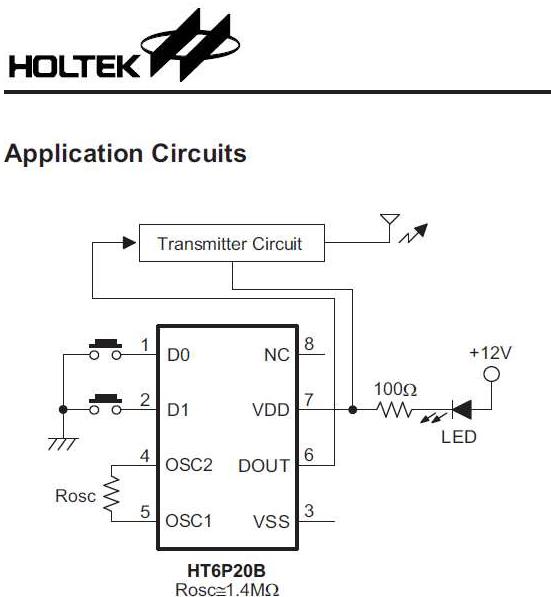
En lisant la DataSheet de l'EV1527 il est alors facile de positionner la ou les sondes de l'analyseur logique ou même la sonde de l'oscilloscope et d'observer. Voici leurs emplacements possibles pour observer ces données :



Voici 3 DataSheets, il y a celle du circuit de la clé utilisée dans ce document, mais aussi 2 autres qui peuvent présenter de l'intérêt en fonction du modèle de clé dont vous disposez mais pas seulement. Je vous laisse fouiller dedans, ouf elles ne sont pas très épaisses :

- SC2240B.pdf
- HT6P20B.pdf
- EV1527.pdf

Le document PDF relatif HT6P20B (Attention à l'implantation des Pins qui est différente) nous présente quelques schémas d'application possible de ce type circuit (EV1527...). Et cet extrait semble parfaitement correspondre à notre cas de figure.



Ces documents nous disent qu'il s'agit d'un encoder OTP.

Alors attention ce n'est pas à confondre avec le célèbre OTP (One Time Pad) utilisé pour chiffrer des messages : [https://en.wikipedia.org/wiki/One-time\\_pad](https://en.wikipedia.org/wiki/One-time_pad)

Là il s'agit du One-Time Programmable qui permet de programmer une donnée dans un composant électronique. Ceux qui ont un doute dans mes propos je vous propose de lire et regarder ceci :

- <https://components101.com/ics/ev1527-encoder-ic-pinout-datasheet-equivalent-circuit-specs>
- <https://www.utmel.com/components/ev1527-encoder-ic-datasheet-pdf-equivalent-and-circuit?id=865>

Alors, j'espère que nous sommes d'accord, il ne s'agit pas de s'emballer et d'imaginer que nous sommes entrain de craquer de l'OTP.

Pour réaliser votre propre système, vous devriez trouver l'essentiel des informations avec ces 2 liens :

- [https://done.land/components/data/datatransmission/wireless/shortrangedevice/am/ask/e\\_v1527/receiver/rx480e-4/](https://done.land/components/data/datatransmission/wireless/shortrangedevice/am/ask/e_v1527/receiver/rx480e-4/)
- <https://www.amazon.fr/QIACHIP-R%C3%A9cepteur-d'apprentissage-t%C3%A9l%C3%A9commande-Ensembles/dp/B0838WXFKJ?th=1>

Il est évident qu'en fouillant sur Aliexpress, il est probablement possible de réduire encore les coûts par rapport à Amazon.

Une autre solution pour le passionné d'électronique consiste à prendre un module ESP32 et lui adjoindre un module CC1101 émettant sur la bande ISM 433 par exemple. C'est ce principe que le chercheur en cybersécurité Joel Serna Moreno utilise pour son projet EvilCrowRF (<https://github.com/joelsernamoreno>). Ce qui a pour avantage de simplifier la programmation en utilisant l'IDE Arduino. Et d'offrir du coup un serveur WEB embarqué autonome traitant les signaux de télécommande sur la bande ISM 433 ou une autre suivant le module employé.

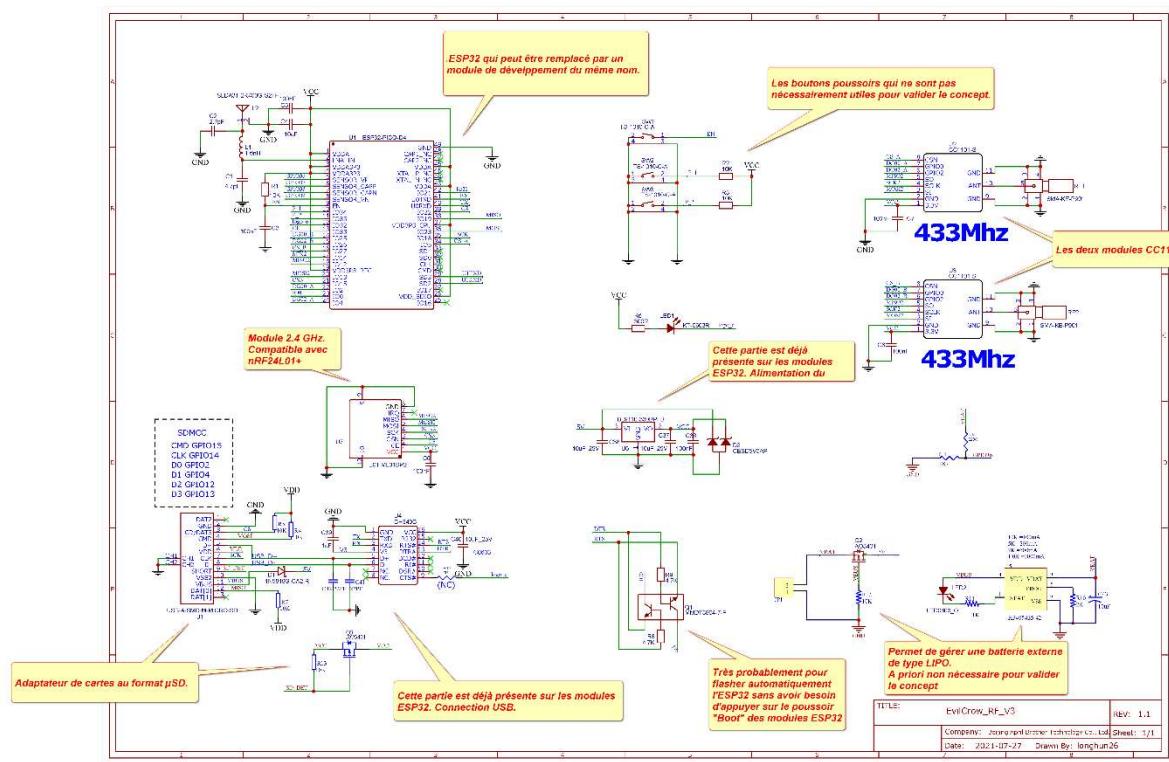
Comme je l'avais écrit en 2018, dans un précédent article, il est tout à fait possible de programmer les modules ESP depuis l'IDE Arduino : <https://pchene.wordpress.com/2018/09/27/magique-esp-wroom-32-et-arduino-ca-marche/>

Si vous faites des recherches sur « h-RAT » vous pourrez constater alors que casser un système de clé à code tournant ou pas est aujourd'hui accessible. Joel Serna Moreno et d'autres l'ont très nettement démontré :

- <https://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/>
- [https://www.youtube.com/watch?v=mdkEK\\_wmWJA](https://www.youtube.com/watch?v=mdkEK_wmWJA)
- [https://github.com/h-RAT/EvilCrowRF\\_Custom\\_Firmware\\_CC1101\\_FlipperZero/tree/main](https://github.com/h-RAT/EvilCrowRF_Custom_Firmware_CC1101_FlipperZero/tree/main)
- ...

Par expérience, j'ai pu constater que le couple EvilCrowRF v2 et h-RAT est particulièrement étonnant en termes de résultats. Les commandes à distance de serrures qu'elles soient à code tournant ou pas lui offre peu/pas de résistance en très peu de temps de mise en œuvre.

Ici le schéma de la version V3 du EvilCrowRF, le cœur du projet est un ESP32 qui vient communiquer avec 2 modules CC1101. Puis on y trouve la gestion d'une carte microSD (pour enregistrer les données des captures ou à jouer, puis le code HTML de l'application HTML et les fichiers de configuration de l'application) :



Pour celui qui le désire, avec peu de recherche sur internet, il est aisément de trouver ce schéma et d'autres informations concernant le hardware tout comme les sources du logiciel du projet EvilCrowRF. Les notes d'application et datasheets des différents modules utilisés termineront d'aider à la réalisation d'une telle intégration électronique.

Donc en mettant un tant soit peu les mains dans le cambouis, il est possible pour un diablotin de la cybersécurité d'ouvrir et même fermer de nombreuses serrures commandées à distance et ceci sans passer nécessairement par un outil commercial comme le FlipperZero ou autre.

## Conclusions

En fait, je vais tirer 3 conclusions, elles sont les suivantes, car je souhaite vous faire partager 3 retours d'expériences qui sont finalement distincts :

- Conclusion sur le HackRF
- Conclusion sur la suite Universal Radio Hacker
- Conclusion sur cette faille du système de télécommande

### Conclusion sur le HackRF

Le HackRF est une solution open source d'émetteur récepteur SDR permettant d'émettre et recevoir jusqu'à 6GHz. L'un de mes HackRF est équipé d'une carte Portapack. Ils fonctionnent tous les deux constamment H24 et ceci depuis plusieurs années afin de logger des données numériques sur une carte microSD et ils me donnent entièrement satisfaction ... La version de la carte HackRF date de 2014, soit il y a 10 ans. Je peux toujours la mettre à jour.

Initialement, c'est une carte de développement pour le domaine des radiofréquences et non un équipement SDR comme peut l'être un transceiver FlexRadio par exemple. Tant dans des activités de cybersécurité, de développement, de mesure, d'amateur radio, équipé ou pas de la carte Portapack, c'est un formidable outil qui n'a pas de concurrence lui arrivant à la cheville si l'aspect coût est une priorité.

### Conclusion sur la suite logicielle Universal Radio Hacker

Là aussi, c'est une solution open source sans équivalent à ma connaissance. Toutes les fonctions essentielles à des activités de hack des systèmes radio numériques sont présentes. On peut identifier, analyser, forger, simuler ou émettre un signal radio numérique de manière simple et ergonomique pour celui qui possède à minima quelques bases sur les signaux numériques. C'est une solution logicielle qui évolue régulièrement. Elle est « un couteau suisse » du hack offensif ou défensif. C'est un outil qui peut tout à fait convenir au hacker, à l'amateur des signaux numériques, à l'enseignant et à ses élèves, au chercheur, au professionnel ou passionné du SIGINT (SIGnals INTElligence) et du COMINT (COMMunications INTElligence). URH est et sera très probablement un outil à suivre, à posséder, à utiliser...

### Conclusion sur cette faille du système de télécommande

L'absence de fiabilité en termes de sécurité repose en grande partie sur le fait qu'il n'y a pas de dialogue entre la clé et le bloc de réception. Ce dernier se contente uniquement de recevoir. La clé a le bon identifiant et ça s'arrête là. D'où la facilité d'attaque par un enregistrement du signal et de le rejouer. La donnée transmise par les airs radio contient un identifiant et une commande à exécuter. Il est alors facile de se moquer de la sécurité très relative de ce genre de produit. On utilise alors URH ou autre outil comme un perroquet et encore celui-ci est probablement plus intelligent (l'oiseau). La crédulité, la méconnaissance, l'innocence de l'utilisateur l'expose comme bien souvent à des surprises désagréables voir plus.

Une seule fréquence de transmission est utilisée, là aussi ça facilite grandement les choses. Dans le cas d'un échange entre la clé et le bloc de réception ou pourrait imaginer un changement de fréquences d'émission/réception durant le dialogue (dans le jargon technique : FHSS - Frequency Hopping Spread Spectrum) ce qui compliquerait l'écoute clandestine.

## Sans verser dans la paranoïa mais à méditer

Selon les dires de mon fils Viktor, il connaissait le FlipperZero avant que nous parlions de tout cela. Sa source d'information sur cette solution sont les nombreuses vidéos disponibles sur TikTok.

Il me semble qu'il serait bon de s'interroger sur l'éducation de nos enfants à ces solutions prêtées à l'emploi pour mettre à mal de nombreux systèmes dits sécurisés.

La sécurité cyber ou pas est avant tout, je crois, une affaire de communication au moins dans le domaine de la prévention. Il est dommage que cette prévention ne soit pas ou peu faite dès le plus jeune âge afin que les risques et conséquences associées soient conscientisés par les victimes potentielles comme par les potentiels auteurs d'actes malveillants.

Une personne malveillante équipée d'un outil comme le EvilCrowRF (moins de 40 euros) peut ouvrir portes et coffre de la plupart des automobiles, camping-car mais aussi s'autoriser l'accès à une propriété, un parking, un garage... en un rien de temps.

Pour en revenir aux véhicules, laisser des objets de valeur à l'intérieur de celui-ci, c'est clairement prendre un risque au regard du vol et en plus il n'y aura aucune trace d'effraction (ça va être compliqué pour la déclaration, l'assurance...).

Idem pour le cas où un individu voudrait se cacher dans le véhicule pour de multiples raisons (fuite, agression, y cacher un objet ...)

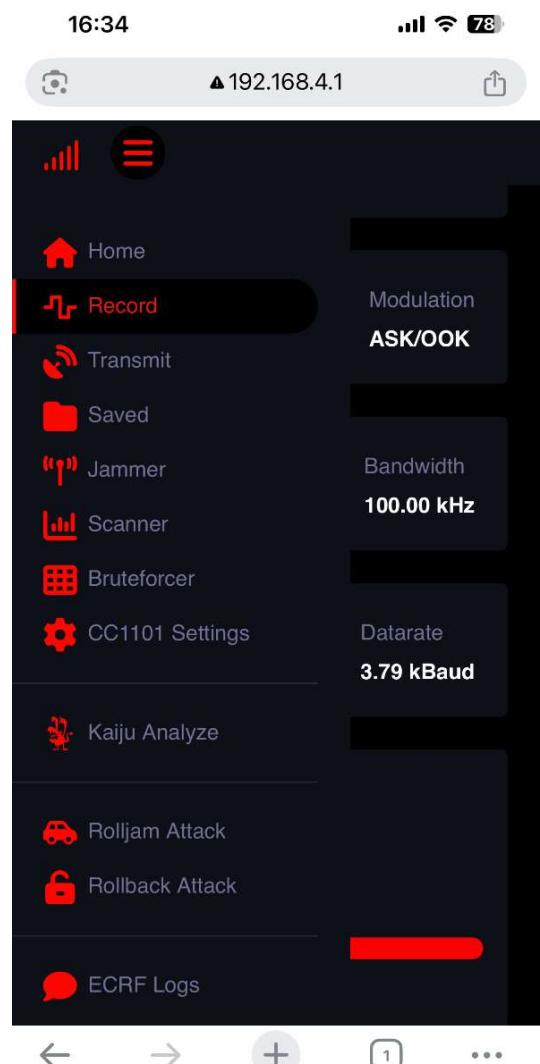
Imaginer sécuriser une porte de garage communiquant sans sécurité avec une habitation avec ce type de clé, c'est là aussi prendre des risques. Là aussi, c'est sans trace d'effraction.

Laisser une telle clé sans fil en évidence sur son bureau, lors d'une soirée..., elle est duplifiable en toute discréption en une fraction de seconde par quelqu'un de mal attentionné.

Avec un HackRF c'est juste moins discret car il faudra un ordinateur ou éventuellement avec sa carte fille Portapack mais un EvilCrowRF ou un FlipperZero, ça tient dans un paquet de cigarettes.

Un EvilCrowRF se manipule depuis un téléphone portable (tablette, ordinateur...) donc pour la discréption de la manipulation c'est idéal en ces temps où tout le monde ou presque a un téléphone portable collé à la main. L'EvilCrowRF se trouve alors dans une poche, petit sac à dos...

La distance d'opération de l'acte d'ouverture ou même lors du repérage (pour faire un double par exemple) peut être plus ou moins éloignée en fonction de l'antenne employée.



Depuis Google Chrome avec un iPhone :  
Le serveur h-RAT embarqué sur un  
EvilCrowRF v2. Attaques, captures... sont  
sauvegardées sur la carte microSD de  
l'EvilCrowRF et téléchargeable sur le  
mobile...

## Pour aller plus loin

Si vous ne savez pas comment occuper vos soirées, nuits et même journées pour les prochaines années 😊, voici quelques liens qui combleront cela. C'est particulièrement vrai dans la section « A l'écoute des signaux numériques ».

- Le logiciel Universal Radio Hacker dans la version 2.9.2, utile pour ceux qui se trouvent sous Windows 7 car les versions récentes ne fonctionnent pas. Cette version-là se trouve ici sur le GitHub du logiciel :  
<https://github.com/jopohl/urh/releases/download/v2.9.2/Universal.Radio.Hacker-2.9.2-x64.exe>
- Autres instruments de mesure des RF qui cohabitent avec l'analyseur de spectre. Ici un document en anglais qui fait un comparatif de mesures entre un SNA et un VNA :  
<https://www.keysight.com/us/en/assets/7018-02338/technical-overviews-archived/5990-4798.pdf>

## Initiation aux modulations numériques et codages

- Les modulations numériques :  
[https://deptinfo.cnam.fr/Enseignement/Memoires/LUSTEAU.Franck/Pages/Les\\_modulations\\_de\\_base.htm](https://deptinfo.cnam.fr/Enseignement/Memoires/LUSTEAU.Franck/Pages/Les_modulations_de_base.htm)
- Les coder l'information transmise par la modulation :  
[https://deptinfo.cnam.fr/Enseignement/Memoires/LUSTEAU.Franck/Pages/Les\\_codages.htm](https://deptinfo.cnam.fr/Enseignement/Memoires/LUSTEAU.Franck/Pages/Les_codages.htm)
- Techniques de modulation numérique :  
<https://www.geeksforgeeks.org/digital-modulation-techniques/>
- En anglais : Exploring communications technology :  
<https://www.open.edu/openlearn/digital-computing/exploring-communications-technology/content-section-0?active-tab=content-tab>

## Quelques usages du HackRF One

- Le HackRF One en analyseur de spectre jusqu'à 7GHz :  
<https://github.com/pavsa/hackrf-spectrum-analyzer>
- Le logiciel d'analyse spectrale Satsagen qui est utilisé dans ce document et qui me donne entière satisfaction quand je suis amené à l'utiliser :  
<https://www.albfer.com/en/2020/02/21/satsagen-2/>
- Un exemple d'usage du HackRF One sur une liaison montante et descendante d'un satellite radioamateur (QO 100) :  
<https://f1atb.fr/fr/emetteur-et-recepteur-vers-qo-100-avec-2-hackrf/>
- Le blog d'Oleg Kutkov qui réalise des projets à base de HackRF qui méritent le détour :  
<https://olegkutkov.me/>

## Cybersécurité et communication sans fil

- Pour ceux qui souhaitent approfondir sérieusement ce monde de la sécurité des systèmes sans fil, je vous conseil de vous rendre sur cette page GitHub qui dresse un panorama de solutions mais pas que relativement complet de solutions pour l'amateur averti, le

chercheur... :

<https://github.com/cn0xroot/RFSec-ToolKit/blob/master/README.md>

- Les éditions Diamond publient régulièrement la revue MISC sur la cybersécurité (traitée sérieusement), le sujet des radiocommunications y est régulièrement abordé. Il y a eu un document célèbre publié dans cette revue, document qui montre comment intercepter Texto et plus de nos téléphones portables : [https://boutique.ed-diamond.com/7\\_misc](https://boutique.ed-diamond.com/7_misc)  
L'article a été publié en 2017 et est toujours d'actualité donc là aussi la sécurité des échanges avec un mobile est toute relative :  
<https://connect.ed-diamond.com/MISC/mischs-016/interception-passive-et-decodage-de-flux-gsm-avec-gr-gsm>
- GNU Radio est un outil de développement d'applications SDR, il prend en charge le HackRF One mais aussi les clé RTL-SDR. Ce logiciel est devenu une référence, de nombreux tutos existent sur Internet : <https://www.gnuradio.org>
- La suite logicielle Radioconda qui permet de faire tourner GNU Radio mais pas que sous Windows. L'excuse de ne pas avoir un ordinateur sous Linux ne tient plus la route pour s'y mettre 😊 : <https://github.com/ryanvolz/radioconda>
- Le logiciel rtl-433 est un décodeur de nombreux protocoles de produits communicants sur les bandes ISM. On y trouve des produits Lidl, des stations météo Oregon ou Lacrosse, les systèmes pour la pression des pneus TPMS Toyota Renault Citroën..., les systèmes ANT ou ANT+, des unités de control de Jacuzzi et de très nombreux autres produits :  
[https://github.com/merbanan/rtl\\_433](https://github.com/merbanan/rtl_433)

## A l'écoute des signaux numériques

- Artemis est la base de données sur les modulations numérique à avoir, me semble-t-il, si vous êtes passionné par les ondes radio et les différentes modulations qu'on peut y rencontrer. Sans être pour autant exhaustive, cette base de données reste tout de même un superbe outil très complet, mis à jour régulièrement. Vous allez pouvoir explorer les nombreux descendants de ces 4 familles de modulation citées en début d'document :  
<https://www.aresvalley.com/>
- J'affectionne particulièrement SDR-Console qui est un logiciel permettant de piloter entre autres le HackRF One et les RTL-SDR: <https://www.sdr-radio.com/console>
- Il y a aussi SDR Angel qui prend en charge le HackRF One et d'autres cartes SDR. Il est assez incroyable dans ses applications possibles, ne pas hésiter à regarder les démos :  
<https://www.sdrangel.org/>
- SDR # souvent nommé ici et là mais finalement « bof bof » pour mon usage. D'autant que les plugins tant recherchés par certains fonctionnent parfaitement dans SDR-Console :  
<https://airspy.com/download/>
- Pour celui qui veut prendre le temps, il y a SDR Trunk qui peut être très utile et qui vaut vraiment le détour : <https://github.com/DSheirer/sdrtrunk>
- Dans un jus très similaire, il y a OpenEar, je ne donne pas le lien de téléchargement volontairement, l'explication est là :  
<https://www rtl-sdr com/openeear-now-supports-tetra-dmr-pocsag-ads-b/>
- Un outil comme Sorcerer peut aussi aider à démoduler certaines de ces modulations, il est disponible ici et ressemble étrangement à Krypto 500 un logiciel très orienté professionnel du renseignement (COMINT, SIGINT...) :  
<https://www.kd0cq.com/2013/07/sorcerer-decoder-download/>

- Krypto 500 ou 1000, juste pour les yeux à priori car le coût est loin d'être négligeable pour l'amateur. Mais dans la partie « Resources » de Comint Consulting, il y a des documents PDF qui valent le détour : <https://www.comintconsulting.com/>
- Multipsk même si son interface est toujours dans le jus de ses débuts (MS/DOS des années 80) : [http://f6cte.free.fr/index\\_francais.htm](http://f6cte.free.fr/index_francais.htm)
- A voir aussi la documentation de la société Wavecom, un spécialiste de la démodulation numérique pour les écoutes professionnelles (SIGINT COMINT...). Plusieurs documents intéressants ici : <https://www.wavecom.ch/advanced-protocols.php>
- Pour rediriger l'audio du logiciel SDR vers ces logiciels de démodulation numérique, il y a des câbles virtuels comme celui-ci par exemple : <https://vb-audio.com/Cable/>
- Voir aussi ce site qui aborde le sujet des câbles virtuels : <https://www.f4hxn.fr/logiciels-cable-audio-virtuel/>

## Quelques points de contraintes et/ou obligations sur les radios transmissions

Ecoutez, en France, une fréquence n'a rien d'illégal. En diffuser son contenu est légalement problématique !

Attention : Cette affirmation vaut aussi pour la diffusion d'un contenu émis par un « pirate ».

Emettre sur une fréquence par contre peut poser un problème légal selon la partie du spectre RF occupée et aussi le moyen utilisé (à ne pas oublier) : Attribution, puissance rayonnée, équipement homologué, antenne et son support ...

Et pour certains équipements comme les brouilleurs (jammer...) là c'est interdiction totale sauf quelques très rares cas de dérogation particulièrement encadrés. La loi interdit les brouilleurs radioélectriques : importation, publicité, cession à titre gratuit ou onéreux, mise en circulation, installation, détention et utilisation (document L.33-3-1 du Code des Postes et communications électroniques). (<https://www.anfr.fr/liste-actualites/actualite/les-enquetes-de-lanfr-les-dents-le-brouilleur-et-au-lit>)

Même si une impression que c'est le « pas vue pas pris » qui semble être la règle. Attention, il y a aussi le « dénoncé » qui peut s'appliquer à ne pas confondre avec la délation.

La surveillance du spectre est une réalité, y compris en France. Même si les actions de sanction semblent quasi-inexistante. Ce n'est pas parce qu'on n'est pas au courant que ça n'existe pas.

Sachez que le monde des radiofréquences est particulièrement règlementé, structuré à l'échelle de la France, de l'Europe, mais aussi du monde. La structure de l'organisation des fréquences à considérer en France est la suivante :

- Le « maître du jeu » au niveau international est l'ITU (International Telecommunication Union). Chaque pays, y adhérant, palabre, réfléchi, décide... sur l'usage des fréquences radioélectriques avec une vue internationale. Les ondes ne s'arrêtent pas aux frontières comme un certain nuage 😊 :

<https://www.itu.int/fr/Pages/default.aspx#/fr>

- Au niveau Européen nous avons l'ETSI (European Telecommunications Standards Institute) qui produit, entre autres, les normes permettant d'assurer la conformité des

équipements radioélectriques. Plus largement, la mission de l'ETSI est de fournir des plateformes où les parties intéressées se réunissent et collaborent au développement et à la promotion de normes pour les systèmes et services des technologies de l'information et de la communication (TIC), utilisées à l'échelle mondiale pour le bénéfice de tous :

<https://www.etsi.org/>

- Sur le sol français France, nous avons l'Arcom : L'Arcom est l'Autorité de régulation de la communication audiovisuelle et numérique. Elle est garante de la liberté de communication et veille au financement de la création audiovisuelle et à la protection des droits. Sa régulation s'étend aux plateformes en ligne – réseaux sociaux, moteurs de recherche... :

<https://www.arcom.fr>

- Nous avons aussi l'ANFR bien connue des radioamateurs (licence, autorisation...), qui dispose des moyens pour retrouver les perturbateurs de tous poils. Sa mission est la suivante : L'Agence nationale des fréquences prépare, coordonne et défend les positions françaises dans les enceintes internationales traitant de politique et d'harmonisation des fréquences, sur l'ensemble du spectre.

<https://www.anfr.fr>

- Les décisions applicables en France apparaissent dans le JO (Journal Officiel). Il publie les textes législatifs et réglementaires de la République française. Toutes ces décisions déclinées en droit français sont disponibles sur le site Légifrance. On y trouve par exemple les attributions de fréquences à une entreprise, à une mairie... Donc observer durant des heures le spectre RF pour trouver la fréquence utilisée par telle ou telle entité (autorisée à émettre) sur le sol français n'est donc pas l'urgence première, se rendre sur ce site peut avoir du sens :

<https://www.legifrance.gouv.fr/>

Il y a 2 exemples de particularités d'un point de vue réglementaire : les eaux internationales et l'espace. Ils sont des environnements où les contraintes réglementaires se réduisent en peau de chagrin. Ceci a profité à cette radio pirate « Radio Caroline » et d'autres. Ici quelques informations sur l'histoire étonnante de Radio Caroline :

[https://fr.wikipedia.org/wiki/Radio\\_Caroline](https://fr.wikipedia.org/wiki/Radio_Caroline)

Dans les usages des radiocommunications, on s'exprime parfois en code Q (QSO par exemple) quand on s'adresse à d'autres passionnés de radio, voici de quoi traduire cette codification qui est normalisée par l'ACP131 E, c'est ici :

[https://www.angelfire.com/va3/navy\\_mars/ACP131.pdf](https://www.angelfire.com/va3/navy_mars/ACP131.pdf)

Puis ici, vous aurez quelques éléments de compréhension sur le pourquoi du comment du code Q :

[https://fr.wikipedia.org/wiki/Code\\_Q](https://fr.wikipedia.org/wiki/Code_Q)