Compromission d'une information basse fréquence au travers d'un étage d'alimentation à hacheur Buck

Tristan PECHEREAU [1,2], Benoit GORAL[1], Charles JOUBERT[2], Fabien MIEYEVILLE[2], Bruno ALLARD[3]

[1] THALES SIX GTS France, Avenue du Maréchal Leclerc, 49300 Cholet, France

[2] Universite Claude Bernard Lyon 1, INSA Lyon, Ecole Centrale de Lyon, CNRS, Ampère, UMR5005, 69621Villeurbanne, France

[3] INSA Lyon, Universite Claude Bernard Lyon 1, Ecole Centrale de Lyon, CNRS, Ampère, UMR5005, 69621Villeurbanne, France

RESUME – La tendance à la densification des cartes électroniques est rendue possible grâce à l'utilisation de composants toujours plus miniaturisés et intégrés. Cependant, dans le cas du développement d'un produit traitant de l'information sensible, ces stratégies de densification s'opposent à l'ajout de nombreux composants de filtrage assurant le respect de certaines normes de sécurité de l'information, comme celles connues sous le nom de code "TEMPEST". Dans le cadre de cet article, il sera mis en évidence la possibilité d'observer l'activité d'une carte électronique, sur son alimentation principale, en cas d'absence de filtre, conduisant à un manquement aux normes TEMPEST.

Mots-clés – CEM conduite, TEMPEST, sécurité de l'information, convertisseurs DC/DC.

1. INTRODUCTION

Le développement de produit de communication tactique nécessite de respecter certaines normes, permettant de faire cohabiter au sein de l'équipement de l'information chiffrée et de l'information sensible. Dans les normes TEMPEST, une classification est faite sur les signaux, classés en ROUGE/NOIR selon leur nature et leur criticité. Ainsi, des contraintes sont définies pour la "Séparation des circuits, composants, équipements et systèmes électriques et électroniques qui traitent des informations de sécurité nationale (ROUGE), sous forme électrique, de ceux qui traitent des informations de sécurité non nationales (NOIR) sous la même forme." [1]. Durant le développement d'un équipement répondant aux normes TEMPEST, les zones ROUGEs et NOIREs ont besoin d'être le plus possible séparées physiquement pour éviter les fuites d'information entre les deux zones. Dans chaque zone se trouvent des charges spécifiques, des régulateurs de tension et quelques filtres. Les charges traitant de l'information en clair sont considérées en zone ROUGE car la captation de cette information constituerait une compromission. Lorsque ces informations sont chiffrées, elles sont considérées comme non-sensibles et sont utilisables en zone NOIRE. Les régulateurs de tension qui alimentent les charges ROUGES sont dans le domaine ROUGE, tandis que ceux qui alimentent les charges NOIREs sont dans le domaine NOIR. Le câble d'alimentation principal, étant la plupart du temps accessible en externe par un attaquant potentiel, est toujours considéré en zone NOIRE. La séparation entre les zones ROUGEs et NOIREs dans les étages d'alimentation est assurée par des "filtres TEMPEST", de type passe-bas, entre les régulateurs de tension.

Les normes dites TEMPEST sont les OTAN SDIP-27, SDIP-28 et SDIP-29 et sont en grande partie classifiées. La norme OTAN-SDIP-27 donne la classification des zones de proximité d'un équipement dit TEMPEST, zones qui nécessitent différents niveaux de sécurité. Elles sont nommées Niveaux A, B et C [2], en fonction de la distance séparant l'attaquant de l'appareil cible. Le non respect de ces normes entraîne des risque de fuite vers l'alimentation principale ou les charges noires, par conduction ou rayonnement électromagnétique, illustré figure 1.

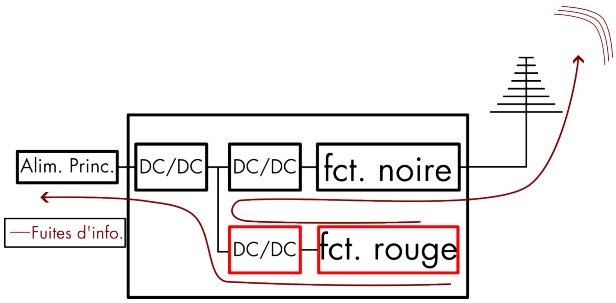

FIG. 1. Fuites possibles du domaine rouge vers le domaine noir

Ces niveaux de classification font que la littérature sur les normes TEMPEST ou les techniques de robustification des cartes vis-à-vis des normes, est relativement pauvre, et presque inexistante concernant les exemples d'attaques directes sur carte électronique. Le cas des fuites d'informations du domaine ROUGE vers une antenne de communication NOIRE se retrouve dans la littérature sous le nom de "Screaming Channel" [3, 4, 5, 6].

L'article proposera un zoom sur la compromission d'une information basse fréquence (du domaine ROUGE) au travers d'un étage d'alimentation à hacheur Buck. L'objectif est d'identifier les informations récupérables sur l'alimentation principale (du domaine NOIR). Une carte électronique est développée pour cette démonstration, traitant de l'information dans la bande audio (20 Hz-20 kHz), lorsqu'aucune protection n'est appliquée vis-à-vis de la norme TEMPEST.

L'article détaillera le démonstrateur dans la section 2, puis montrera des exemples de fuite aux sections 3 à 4 avant d'expliquer la suite du travail.

2. FORMAT DU DÉMONSTRATEUR

Une carte de démonstration de fuites a été développée spécifiquement pour embarquer une méthode de traitement de l'information audio, alimentée par un hacheur Buck, dont le schéma de principe est présenté à la figure 2.

Les fuites par conduction électromagnétique au sein de la carte sont la cible principale, depuis la source de l'information jusqu'à l'alimentation principale de la carte.

Afin de démontrer l'existence de cette compromission, des relevés en fréquence, par analyseur de spectre, ont été réalisés sur le démonstrateur. Ainsi, l'accent est mis sur la corrélation

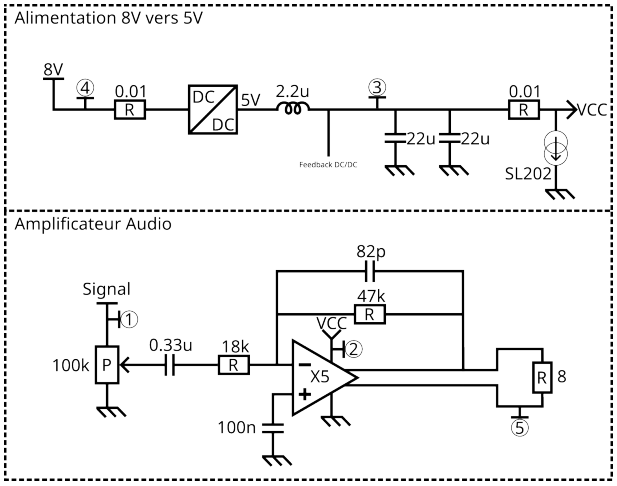

FIG. 2. Schéma simplifié du démonstrateur, alimentation et fonction audio

entre :

- Le signal entrant dans un amplificateur audio et le spectre en tension d'alimentation de l'amplificateur audio (sortie d'un hacheur, alimentant les fonctions sur la carte).
- Le spectre de l'alimentation de l'amplificateur audio et le spectre de la tension d'entrée du hacheur (alimentation générale de la carte).

Par ailleurs, précisons que l'amplificateur utilisé est de classe AB (LM4890) et que le hacheur Buck (LTC3602) est connecté sur une charge active tirant un courant continu de 400 mA pendant toute la durée des relevés, afin de le faire fonctionner en régime continu, quel que soit le signal appliqué sur l'amplificateur.

3. CAPTURE DES FUITES AUDIO

3.1. En Basse Fréquence

Pour simplifier la visualisation des fuites, un simple signal sinusoïdal à 6 kHz et 400 mV crête-à-crête est envoyé sur l'amplificateur audio (repère ① sur la figure 2), dont son analyse spectrale est disponible figure 3.

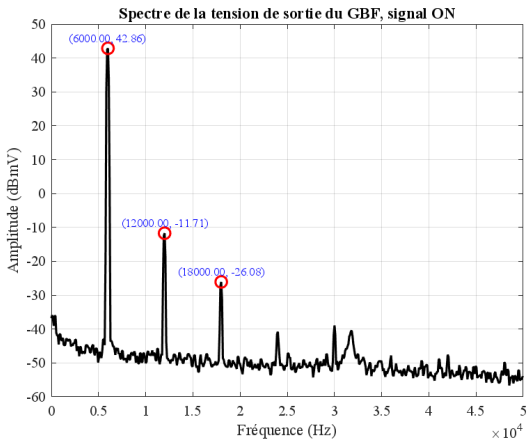

FIG. 3. Spectre du signal envoyé l'amplificateur audio

Il résulte de la structure en classe-AB de l'amplificateur, des fréquences de fonctionnement qui sont de $2n$ fois la fréquence du signal amplifié. Il est alors observable, sur le spectre de la tension de l'alimentation de l'amplificateur audio (repère ② sur la figure 2), des raies à la fréquence de $2n$ fois la fréquence du signal amplifié, soit à 12 kHz et ses multiples.

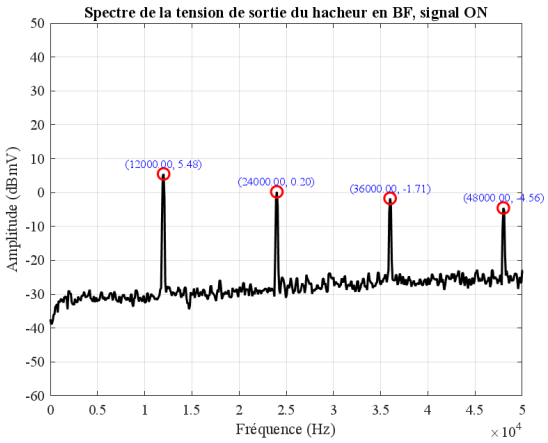

FIG. 4. Spectre de la tension d'alimentation de l'amplificateur audio

Dans l'hypothèse où le fonctionnement interne des composants est connu, il est aisé de retrouver l'information que ces composants traitent sur leurs étages d'alimentation. Cependant, dans le cas d'un espionnage sur l'alimentation d'une carte électronique, le relevé ne se ferait pas sur l'aval du hacheur (sortie ② ou ③), mais sur l'amont (entrée ④). Il est donc plus intéressant de regarder ce dernier, présenté figure 5.

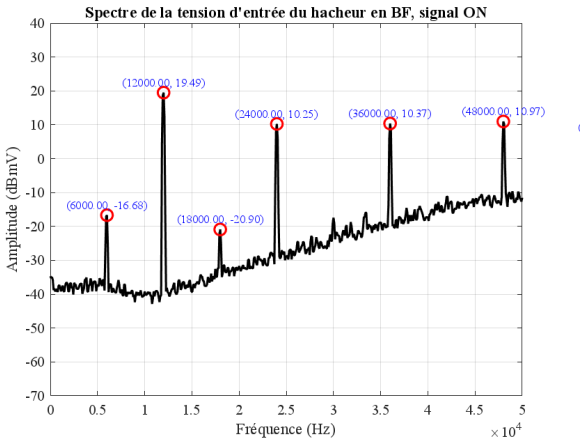

FIG. 5. Spectre de la tension d'entrée du hacheur

Il est notable dans ces relevés que non seulement le convertisseur DC/DC laisse passer toutes les informations basse-fréquence, mais qu'il amplifie également certaines raies. Dans le cas de cette conception proche des recommandations du fournisseur, aucune protection n'est assurée quant à la fuite d'information conduite de la sortie vers l'entrée de ce hacheur Buck.

3.2. Autour de la fréquence de commutation

En ce qui concerne ces fuites d'information, un second phénomène apparaît, qui pourrait être appelé « porteuse non intentionnelle ». Ce phénomène est décrit dans [7], chapitre 3.3, Ils mettent en avant le fait que dans un composant non linéaire utilisant des signaux d'horloge pour fonctionner, il se crée très souvent des modulations parasites de ces signaux d'horloge par l'information traitée par ce même composant. Dans notre cas, ce n'est pas tant le fonctionnement non-linéaire de l'amplificateur qui nous intéresse, mais plutôt la fréquence de commutation du hacheur. Dans l'éventualité où, comme observé juste avant, l'information basse fréquence remonte jusqu'au hacheur, il est

tout à fait probable qu'un phénomène de modulation entre la fréquence de hachage et l'information basse fréquence (le sinus à 6 kHz, transformé en fuite à 12 kHz par l'amplificateur de classe AB) se produise. Le hacheur commutant à 990 kHz, il est intéressant de regarder de plus près ce qui se passe autour de 990 kHz et de ses harmoniques, illustré dans les figures 6 et 7.

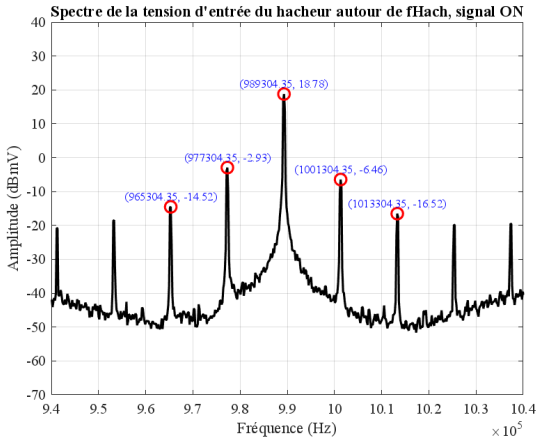

FIG. 6. Spectre de la tension d'entrée du hacheur autour de 1 MHz

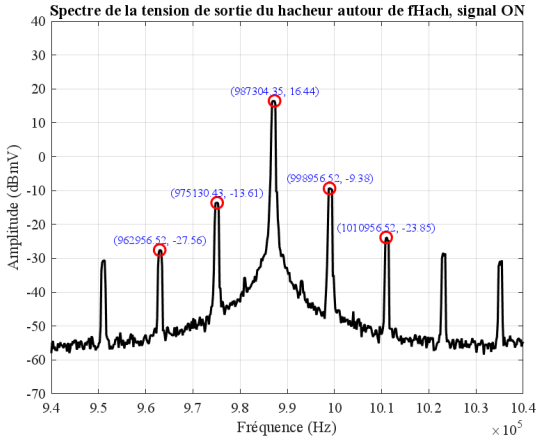

FIG. 7. Spectre de la tension de sortie du hacheur autour de 1 MHz

Le signal de commutation d'un hacheur n'étant pas sinusoïdale, il est imaginable ce même phénomène de modulation non intentionnelle sur les harmoniques du signal de commutation, ainsi illustré aux figures 8 et 9.

En l'occurrence, l'observation fréquentielle de la fréquence de hachage et de sa première harmonique amène à mettre en avant ce phénomène de modulation non intentionnelle sur Fhach et ses harmoniques. Malheureusement, et encore une fois pour ces relevés en plus hautes fréquences, les raies ne sont pas atténuées mais amplifiées. Dans la configuration actuelle et pour ces fréquences, il n'est pas possible d'exploiter ce hacheur buck pour apporter un filtrage supplémentaire.

Par ailleurs, au même titre que dans [7] avec les horloges internes, l'observation du signal temporel de la tension d'entrée du DC/DC, figure 10, met en avant très clairement la présence de cette modulation de la tension d'entrée avec un signal à 12 kHz.

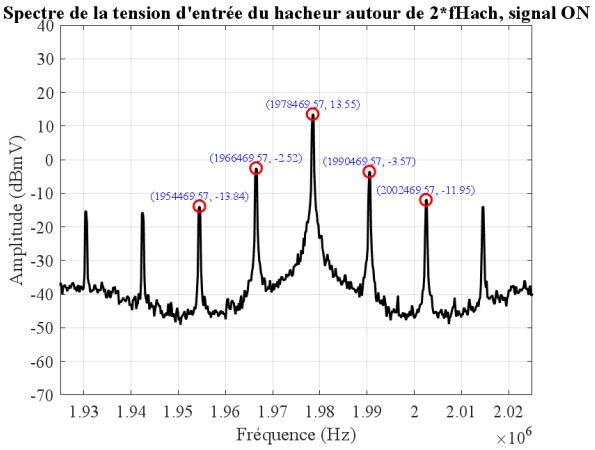

FIG. 8. Spectre de la tension d'entrée du hacheur autour de 2 MHz

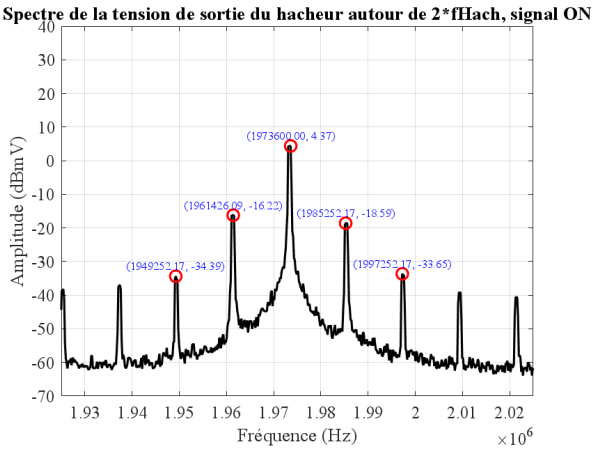

FIG. 9. Spectre de la tension de sortie du hacheur autour de 2 MHz

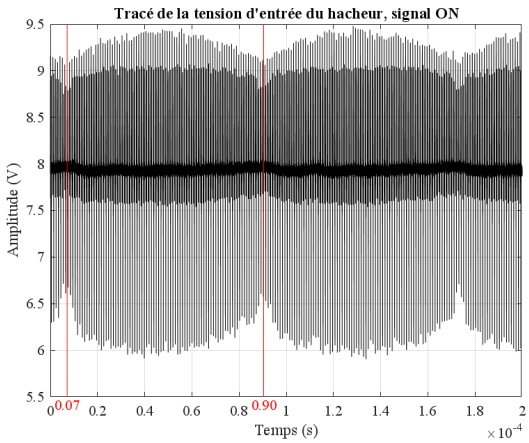

FIG. 10. Visualisation temporelle du signal d'entrée du hacheur

3.3. *Application plus réaliste : Espionnage de l'alimentation générale*

Pour la mise en place d'une attaque plus réaliste, l'espionnage de l'activité de l'alimentation d'une carte se fait par "reniflement" sur les fils d'alimentation de cette carte par une simple sonde de courant. Concernant cette nouvelle application, les conditions d'essai sont les mêmes que sur l'analyse des tensions de fonctionnement, décrites dans le chapitre 2.

Ainsi, en observant les transformé de fourrier à l'oscilloscope des courants d'entrée et de sortie relevés par champs proche sur les fils d'alimentation, tracés figures 11 et 12 il est encore plus aisé de lié l'activité de la carte à l'analyse de son alimentation.

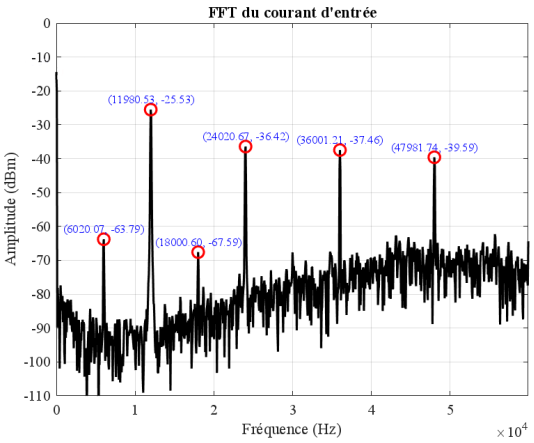

FIG. 11. FFT sur le courant d'entrée du démonstrateur

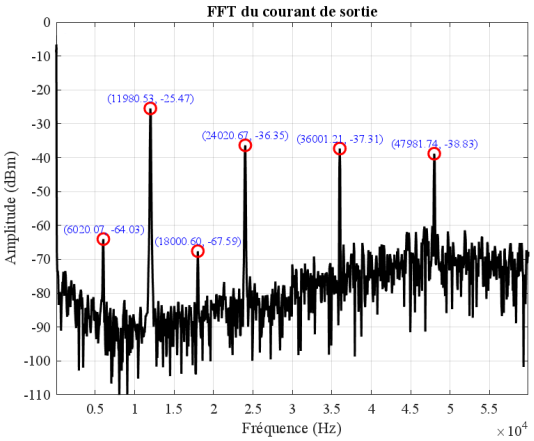

FIG. 12. FFT sur le courant de sortie du démonstrateur

Il est notable que l'analyse sur les courants donne des résultats encore plus clair que les relevés directs des tensions sur carte, que ce soit directement sur la fondamentale du signal traité (première raie à 6 kHz) ou sur les fréquences de fonctionnement de l'amplificateur de classe AB. Toutefois, il est bien évidemment simple de retrouver l'information que nous souhaitons espionner, lorsque nous connaissons l'information à capturer. Une évolution de ces travaux serait de créer des modèles "boites noires", ainsi qu'un dispositif de capture d'activité sur l'alimentation de ces modèles. Cette évolution permettrait une approche plus réaliste de ces captures d'informations et mettrait plus en évidence ces compromissions d'informations.

4. OUVERTURE : COMPROMISSION D'UN BUS SPI SUR MICRO-CONTRÔLEUR STM32

Dans le cadre de l'étude de ces fuites par conduction électromagnétique, ce n'est pas seulement les informations basse fréquence type audio qui sont susceptible d'intéresser un attaquant potentiel, mais aussi les informations numériques de plus hautes fréquences (SPI, UART, Ethernet ...). Le démonstrateur développé embarque, en plus de la fonction audio, un Micro-Contrôleur STM32-L432KC afin de mettre en avant ces fuites numériques. Dans la manipulation suivante, la sortie du hacheur n'est pas reliée à une charge active, il fonctionne donc en régime discontinu, la stabilisation de la fréquence de hachage n'étant pas nécessaire.

Ainsi, dans un premier temps et pour faire une ouverture sur la suite des travaux que sera l'étude spécifique des fuites d'information des communications numériques, Un montage simple est effectué en sortie du bus SPI du STM32, figure 13, alimenté par le hacheur LTC3602.

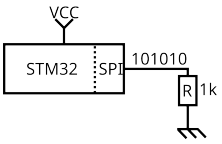

FIG. 13. Schéma simplifié du démonstrateur, communication SPI

Pour rendre la visualisation de ces fuites la plus évidente possible, un caractère "*" est envoyé sur le bus SPI, puisque son code ASCII est le suivant : 101010. Se traduisant donc par une série d'état haut (3.3 V) et d'état bas (0 V) sur la sortie SPI. Cette dernière étant relié à une simple résistance de 1 kΩ, les appels de courant sont donc de valeur faible, 3.3 mA. La visualisation de l'information numérique envoyé sur le bus SPI est disponible figure 15.

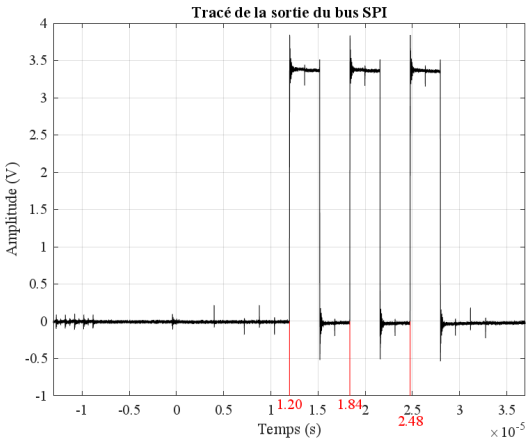

FIG. 14. Sortie du bus SPI

Au même titre que pour l'étude des fuites audios, il est intéressant d'observer l'entrée du convertisseur continu-continu, et vérifier la corrélation entre l'information transitant sur le bus SPI et les perturbation sur la ligne d'alimentation principale. Cette observation est disponible figure 15.

Il est remarquable une corrélation entre les légers pics de tension (environ 0.1V Crête-Crête pour le passage à l'état haut, environ moitié moins pour le passage à l'état bas) et les changements d'état de la sortie SPI. Ainsi, bien que cette perturbation soit de relativement faible valeur, elle permettrait, en théorie, de relier l'activité numérique de la carte à la consommation sur l'alimentation. Les signaux observable de -1.5×10^{-5} s à environ 0.85×10^{-5} s ne sont qu'une image du moment de la commutation de la sortie du hacheur. La suite des travaux concernant cette étude des fuites numériques consistera à étudier plus spécifiquement, sur des signaux plus complexes et sur d'autres canaux de communications la possibilité de reconstruire l'activité d'une carte électronique numérique, toujours grâce à l'activité de son alimentation.

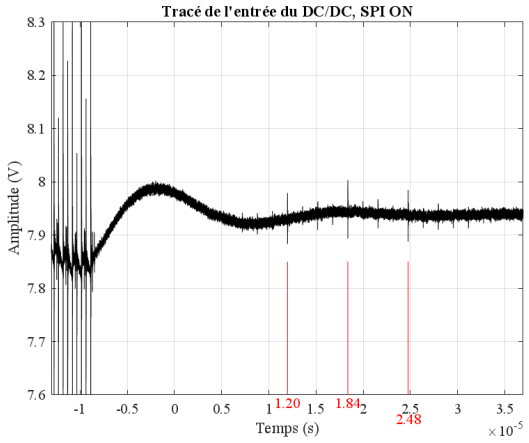

FIG. 15. Visualisation temporelle du signal d'entrée du hacheur, bus SPI en fonctionnement

5. CONCLUSION

La carte étudiée pour la présentation de ces fuites est totalement dépourvue de méthode de filtrage spécifique et se rapproche donc d'une conception classique de carte électronique. Dans le cas d'une application grand public, nous pouvons constater que l'information transitant sur des étages de traitement de données se retrouve en clair sur la ligne d'alimentation, qui rappelons-le, est considérée dans le domaine NOIR car attaquable directement par méthode de "reniflement", c'est-à-dire, avec une simple sonde de courant ou de tension.

Un module de traitement d'information couplé à une méthode d'attaque permettrait de retrouver les informations transitant sur la carte attaquée, uniquement avec l'activité de l'alimentation. Ces résultats mettent en avant l'importance de la protection de l'information, particulièrement dans le cas d'attaque sur un équipement tactique de communication.

A court terme, il est prévu de réaliser ces mêmes essais sur de la capture d'information numérique, comme décrit au chapitre 4. A moyen terme, des modifications du schéma de l'alimentation électrique devront être expérimentées pour leurrer l'observation du courant et de la tension à l'entrée du système, mais sans dégrader le rendement du convertisseur ni alourdir son empreinte sur la carte. A plus long termes, des modèles de simulation pour pré-dimensionner et valider ces conceptions d'arbre d'alimentation seront étudiés et développés. C'est l'objet des travaux de thèse.

6. RÉFÉRENCES

[1] National security telecommunications and information systems security. « nstissam tempest/2-95 red/black installation guidance. » 1995.

[2] Agence nationale de la sécurité et des systèmes d'information. « Instruction interministérielle n° 300 relative à la protection contre les signaux compromettant. » 2014.

[3] Camurati, G., et A. Francillon. « Screaming Channels ». In Encyclopedia of Cryptography, Security and Privacy, édité par Sushil Jajodia, Pierangela Samarati, et Moti Yung, 1-4. Berlin, Heidelberg : Springer Berlin Heidelberg, 2023.

[4] Camurati, Giovanni. « Security Threats Emerging from the Interaction Between Digital Activity and Radio Transceiver ». Sorbonne, 2020.

[5] Camurati, Giovanni, Aurélien Francillon, et François-Xavier Standaert. « Understanding Screaming Channels : From a Detailed Analysis to Improved Attacks ». IACR Transactions on Cryptographic Hardware and Embedded Systems, 19 juin 2020, 358-401.

[6] Camurati, Giovanni, Sebastian Poeplau, Marius Muench, Tom Hayes, et Aurélien Francillon. « Screaming Channels : When Electromagnetic Side Channels Meet Radio Transceivers ». In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 163-77. Toronto Canada : ACM, 2018.

[7] A. Alcaras et J-F. Gaeng, "Espionnage électromagnétique, Risques, étude, validation et normes TEMPEST", Techniques de l'ingénieur, Électronique-Photonique | Électronique, février 2024.