*Titre :* Sécurisation des communications sans fils.

*Résumé de 1500 caractères, espaces compris :*

La question de sécurisation des données est actuellement au cœur du débat sociétal, dans un monde où de plus en plus d’appareils sont interconnectés. Vous n’aimeriez certainement pas apprendre que vos conversations téléphoniques peuvent être écoutées ou que vos données de santé transmises par votre montre intelligente soient interceptées.

Dans le cadre de mes travaux de recherche, j’ai développé une théorie permettant de sécuriser les communications sans fil. Lorsqu’on envoie de l’information via une antenne, les ondes vont se propager dans toutes les directions et peuvent donc être interceptées. Elles ne sont intrinsèquement pas sécurisées.

Grâce à cette théorie, l’information envoyée depuis un émetteur (antenne dans la rue, borne WIFI,…) ne sera compréhensible que par le récepteur légitime (téléphone portable, montre connectée,…) mais restera brouillée partout ailleurs.

Lorsqu’on émet des signaux via une antenne, ils nous arriveront de manière aléatoire et à des instants différents, en raison des obstacles qu’ils rencontrent sur leurs trajets (immeubles, véhicules,…). Il s’agit ensuite de tirer profit de ces propriétés physiques pour générer, uniquement entre l’antenne et le récepteur, une signature spécifique sécurisant la communication. Si un appareil malveillant réceptionne les signaux émis par l’antenne, il ne disposera pas de la signature pour pouvoir les interpréter. Cette manière de communiquer garanti ainsi la protection de l’information envoyée.

*Contenu : 1481 caractères espaces compris.*

*Phrase d’accroche :*

Mise au point d’une méthode pionnière permettant de sécuriser la transmission de données sans fils.

*Contenu : 99 caractères espaces compris.*