Développement d'une fonction physique non clonable

De nombreux protocoles de sécurité sont basés sur la connaissance *a priori* d'une clé secrète partagée et suffisamment grande afin de ne pas être identifiée. Le problème de cette approche est que la puissance des ordinateurs augmentant inexorablement, il est nécessaire de régulièrement augmenter la taille de ces clés afin de s'assurer de leur efficacité. De plus, lorsqu'une clé est identifiée, elle peut être recopiée à l'infini et donc être utilisée par n'importe qui. Dans le cas d'objets autonomes (IoT, VANET, etc.), ceci pose problème puisque ces objets n'ont pas forcément une grande capacité de stockage et/ou de calcul, et surtout ils doivent pouvoir être identifiés sans ambiguïté.

Une fonction PUF (pour *Physical Unclonable Function*) est un circuit électronique qui, même s'il est connu, donnera des résultats différents pour chacune de ses implémentations. En effet, tous les composants électroniques ont des réponses différentes à un signal donné. Par exemple, en électronique numérique, le passage d'un 0 à 1 ne se fait pas instantannément, mais suit une courbe qui est différente sur chaque composant. Généralement, quand un ingénieur conçoit un circuit électronique, il s'attache à effacer ses différences afin que tous les circuits suivant le même schéma fournissent la même réponse. Dans le cas de PUF, l'idée est de faire exactement l'inverse en amplifiant au maximum ces variations. De fait, deux implémentations d'un même schéma donneront deux réponses différentes et cette réponse peut alors être considérée comme la signature unique et non reproductible de l'objet.

L'objectif de ce projet est d'identifier des schémas de fonction PUF, éventuellement de proposer des améliorations, et d'en réaliser l'implémentation.

En fin de projet, afin de valider la réalisation, il est demandé de fournir au moins deux implémentations accessibles *via* une connectique de type USB.

Contact : Éric Renault
Email : `eric.renault@esiee.fr`