Sécurisation / protection de composants matériels sur ASIC & FPGA

Le sujet consiste à étudier et redisigner un contrôleur matériel en charge des droits d'utilisation de composants matériels.Le rôle de ce contrôleur est de s'assurer qu'un circuit ne peut être utilisé que par des personnes (ou autres circuits) possédant les droits nécessaires.
La mise en oeuvre de ce type de circuit peu apparaître (1) dans le cadre de la lutte contre le piratage des IP ou l'on désire éviter leur contrefaçon, voir être capable d'identifier la source de la fuite (2) lorsqu'un client souhaite acheter un composant pour lequel il ne souhaite pas bénéficier de l'ensemble des fonctionnalités (3) dans un circuit qui peut être la cible d'attaques matérielles et ou chaque communication et chaque changement doit être sécurisée.
Des travaux ont déjà été réalisé dans le domaine au travers d'un stage l'an dernier ayant amené une version "beta" d'un tel contrôleur. L'objectif est de maintenant reconcevoir ce contrôleur en prenant en considération l'ensemble des primitives de sécurité nécessaires (algorithmes de cryptage différents, taille des clefs, sélection des opérations à sécuriser, etc.).

Le travail consistera à :

– comprendre les différentes protections mises en oeuvre (DRM, tatouage, trames cryptées, etc.),
- comprendre et trouver des IP de cryptographie (DES, AES, TEA, etc…) sur internet,
– designer un nouveau contrôleur matériel plus facilement configurable sous contrainte de surface et de consommation d'énergie,
– concevoir une interface graphique QT/Java permettant de créer/configurer des contrôleurs matériels,
– mesurer les performances du controleur sur différents FPGA /ASICs.
– réaliser un démonstrateur matériel sur FPGA autour d'un processeur (avec ou sans OS)