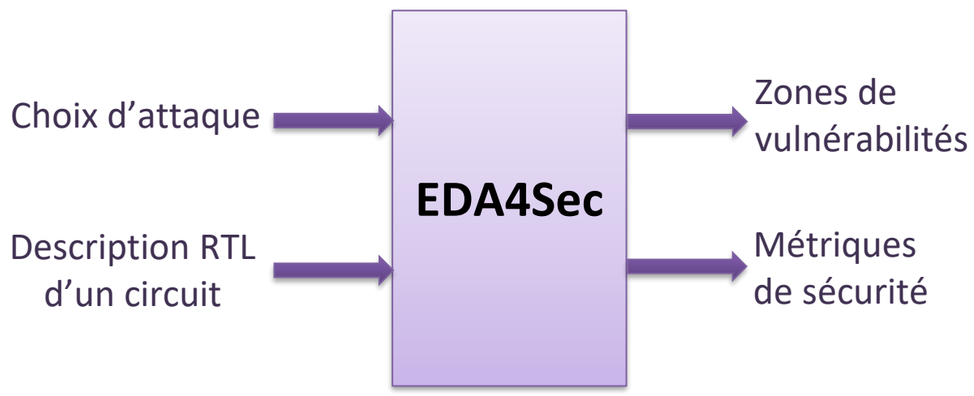
LCIS – EDA4Sec

Outil d'aide à la conception de circuits sécurisés

Auteurs : Marin DAUTREY – Aurélien DELOCHE – Tolga TANER

CONTEXTE ET OBJECTIF

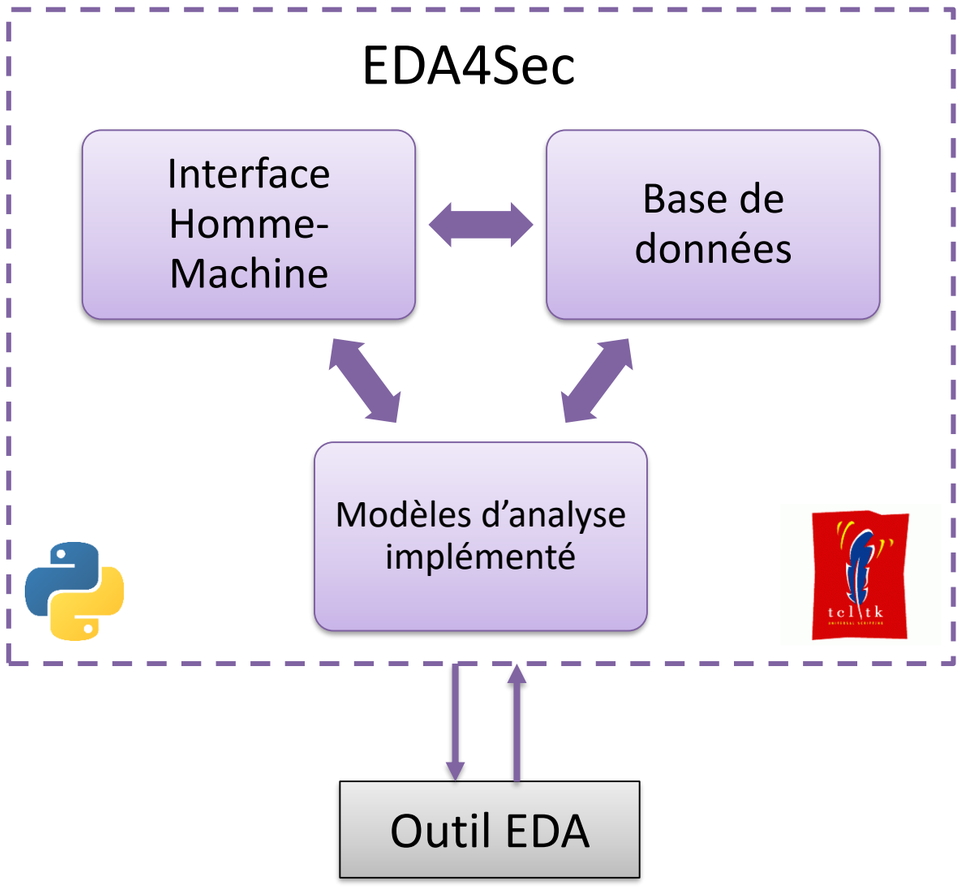
Les problématiques de sécurité matérielle sont de plus en plus importantes pour les concepteurs de **circuits intégrés**. Il est nécessaire de produire un outil pour identifier les vulnérabilités matérielles, qui s'intégrerait dans les flots de conception actuels.



Le projet EDA4Sec est un projet de maturation porté par le **LCIS** et financé par la SATT **Linksium**. Il a pour objectif de développer un logiciel d'analyse de la sécurité des circuits, afin de repérer les potentielles zones sensibles à une attaque matérielle, le tout à partir d'une description RTL et pour plusieurs modèles d'attaque.

MÉTHODES ET DÉVELOPPEMENTS

L'équipe projet a produit un logiciel en Python **implémentant des modèles d'attaque**. EDA4Sec exploite les données structurelles des circuits extraites par les logiciels EDA classiques. Une **base de données** contenant les éléments caractéristiques d'un circuit est créée et est ensuite exploitée par le moteur d'analyse de vulnérabilités développé dans le projet. Une IHM permet au designer de facilement identifier les vulnérabilités quantifiées grâce aux métriques produites par le moteur d'analyse. L'ensemble a été conçu pour être modulaire, afin de pouvoir aisément intégrer de nouvelles méthodes d'analyse.

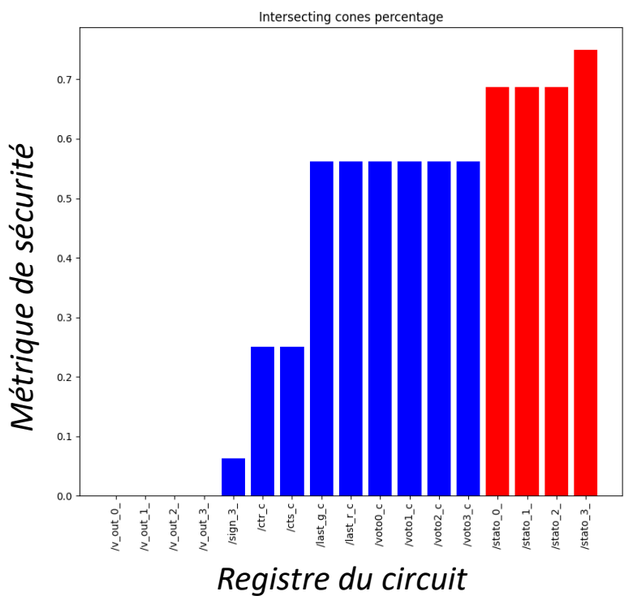


RÉSULTATS ET CONCLUSION

EDA4Sec implémente avec succès différents modèles d'attaque pour automatiser l'identification de vulnérabilités face aux **attaques en faute** (attaque laser, glitch sur l'horloge, glitch sur l'alimentation).

Le logiciel **s'interface aux outils EDA** classiques déjà utilisés par les concepteurs.

EDA4sec apporte des **métriques de sécurité** permettant d'identifier les zones vulnérables d'un circuit. La figure en exemple met en valeur les registres les plus sensibles aux attaques en faute pour un circuit analysé.



MOTS-CLÉS : Sécurité matérielle, outil EDA, conception de circuits intégrés, HDL