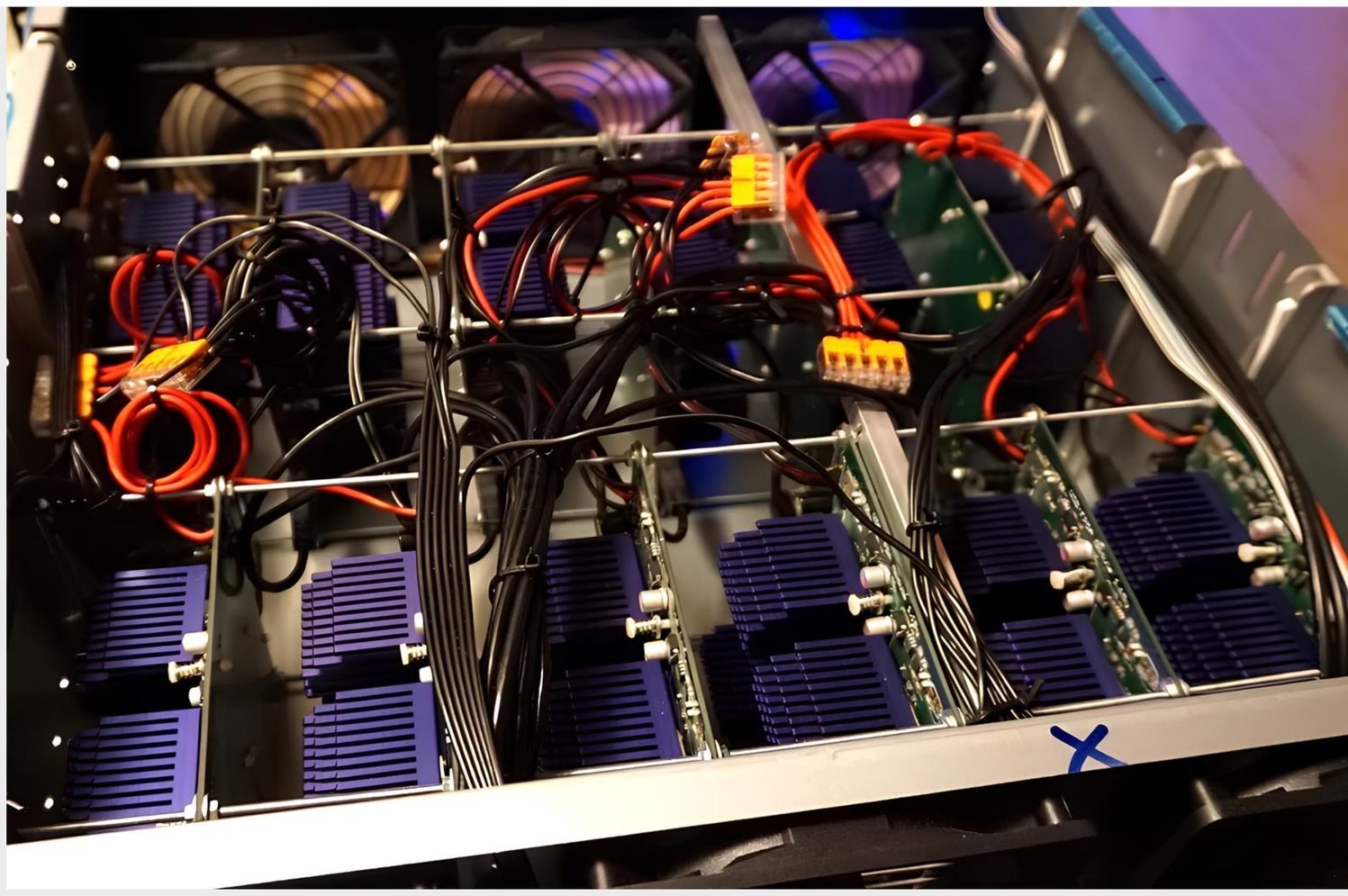
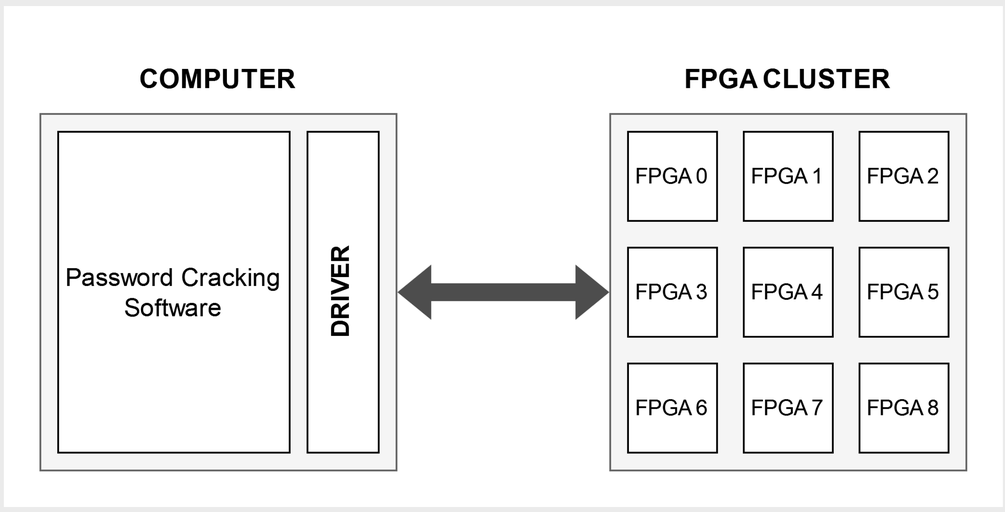
TRAVAIL DE BACHELOR 2024

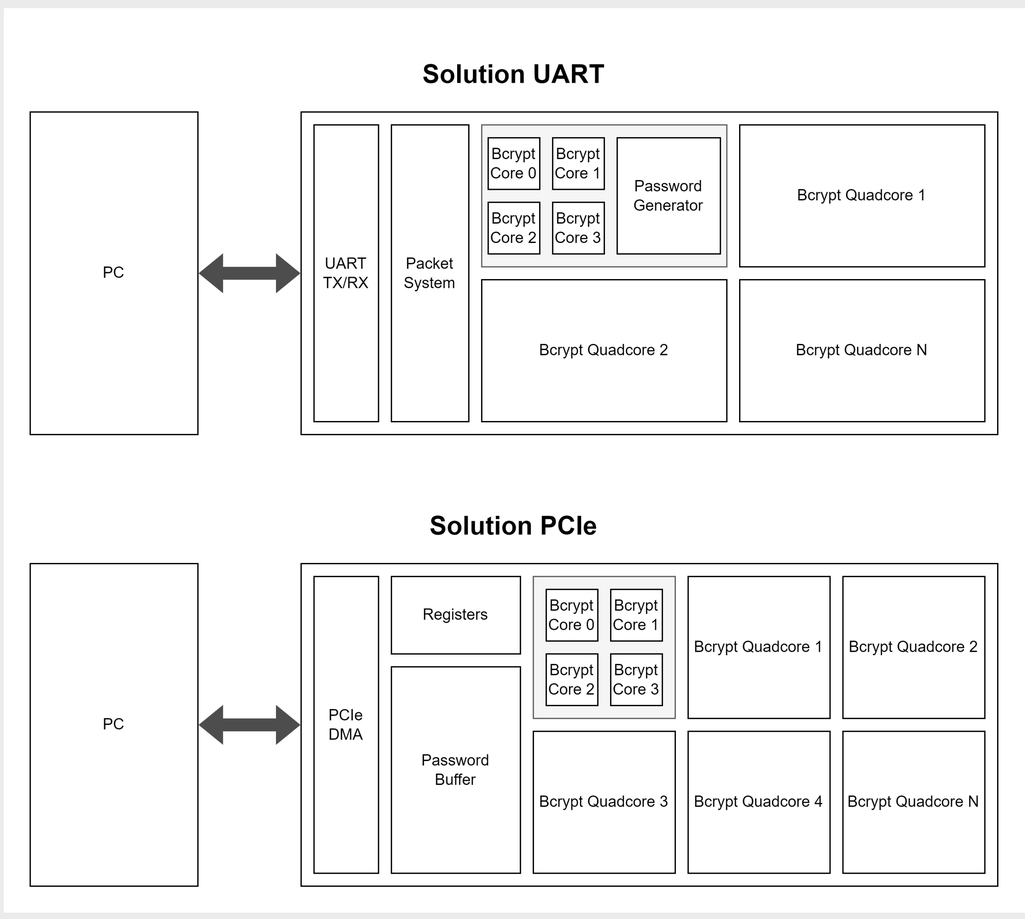
INFORMATIQUE ET SYSTÈMES DE COMMUNICATION

Attaque brute-force sur FPGA pour Bcrypt



Les mots de passe sont sécurisés en utilisant des fonctions de hachage comme Bcrypt, qui ralentit le processus pour rendre les attaques par force brute plus difficiles. Cependant, cette lenteur peut rendre les méthodes traditionnelles de piratage, souvent basées sur des GPU, énergivores et moins efficaces. Ce projet explore l'utilisation d'un FPGA pour accélérer les attaques brute-force contre les mots de passe hachés avec Bcrypt. L'objectif est de concevoir une solution non seulement plus rapide, mais aussi moins énergivore que les approches GPU conventionnelles.





Les tests montrent que la solution FPGA offre une accélération notable tout en consommant beaucoup moins d'énergie que les GPU. Bien que la solution PCIe soit encore en développement, les résultats obtenus jusqu'ici montrent le potentiel des FPGA pour des attaques brute-force plus efficaces et moins énergivores.

Deux solutions sur FPGA, toutes deux utilisant des cœurs de calcul parallèles, ont été développées pour attaquer les mots de passe protégés par Bcrypt. La première méthode génère les mots de passe et calcule les hashs directement sur le FPGA avec plusieurs cœurs parallèles, utilisant une interface UART pour l'interaction utilisateur via des paquets de données.

La seconde méthode, encore en développement, utilise une interface PCIe pour transférer rapidement des mots de passe depuis un ordinateur vers le FPGA. Cette méthode est conçue spécifiquement pour les attaques par dictionnaire, tirant parti de la haute bande passante du PCIe.

Abivarman KANDIAH

Sous la direction de Andrés UPEGUI
En collaboration avec ELCA Security

Hes·so GENÈVE
Haute Ecole Spécialisée de Suisse occidentale

hepia
Haute école du paysage, d'ingénierie et d'architecture de Genève