Examen du 4/2/2010 ENSIMAG/Phelma
Documents de cours autorisés Filière SLE
2h

Sécurité des Systèmes Embarqués

Q1. Que sont les "Critères Communs" ?

Q2. Y-a-t-il une différence importante dans la mise au point d'attaques et de protections selon qu'un processeur cryptographique est implanté dans un circuit précaractérisé ou dans un FPGA configurable par SRAM ?

Q3. Pourquoi les contraintes de test sont-elles un problème important pour les circuits sécurisés ? Donnez au moins deux raisons très différentes.

Q4. Quelle est la différence principale entre une attaque par canaux cachés et une attaque par faute ?

Q5. Résumez le principe de réalisation d'une attaque différentielle en consommation de puissance (DPA).

Q6. Une attaque par faute est-elle réussie dès qu'une erreur a été générée dans le circuit ?

Q7. Les chaînes de scan sont vulnérables aux attaques par fautes : parmi les différentes solutions de protection de ces chaînes, choisissez en une et décrivez-la.

Q8. Résumez les avantages et les inconvénients des codes de détection d'erreurs comme contre-mesure contre l'injection de fautes intentionnelle.

Q9. La redondance temporelle peut être une solution pour la détection d'erreurs : listez les différentes approches pour l'implanter dans un circuit, avec une brève phrase descriptive.

Q10. Le calcul par Double-Data-Rate est une solution possible pour la détection des fautes : quels sont les problèmes les plus importants dont il faut tenir compte lors de l'implantation ?