Sécurité des circuits analogiques

La sécurité des circuits digitaux et des algorithmes de cryptographie est largement publiée

- Pourtant les circuits sont toujours vulnérables!

Les contre-mesures sont nombreuses mais toujours couteuses

- Il faut donc trouver des solutions de sécurité pour les circuits à faible coût.

Dans ce contexte, la sécurité des circuits analogiques doit être envisagée

- Cela commence par une évaluation de ces circuits afin de choisir les contre-mesures les plus efficaces le plus tôt possible pour réduire les coûts de développement en garantissant le meilleur niveau de sécurité possible.

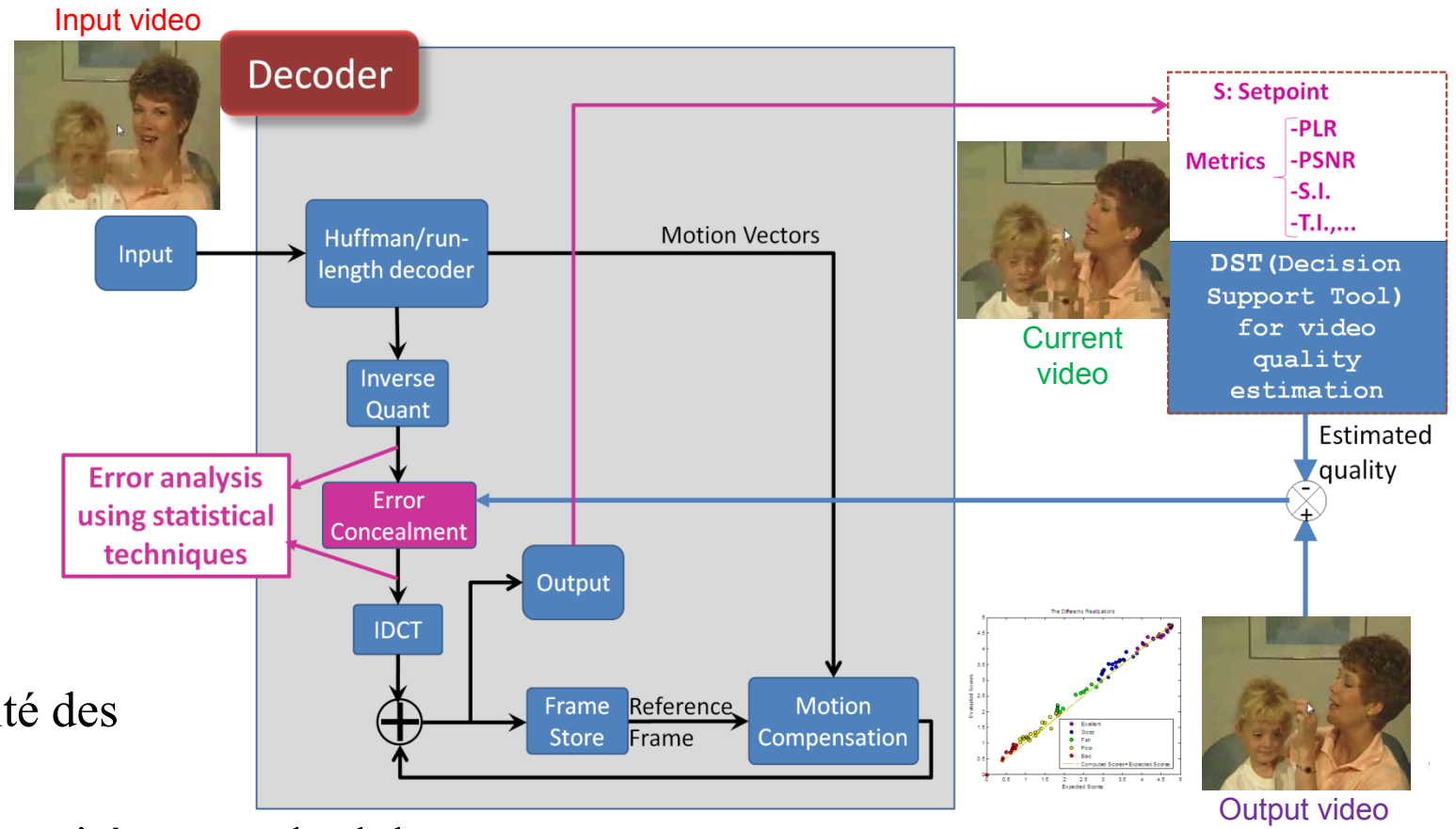
FPGA Emulation of Laser Attacks Against Secure Deep Submicron Integrated Circuits

- Laser attacks pose a threat to ASICs implementing cryptographic algorithms by injecting faults to the circuit's operation
- This fact raises the need to analyze the behaviour of the circuit under laser faults and neutralize them
- Classical approaches of fault injection make use of
  - Fault models not well adapted to laser fault injection
  - Generic Fault injection platforms

  Resulting in:
    - Excessive fault injection durations
    - Simplification of the models
- Goal:
  - Implementation of Laser specific fault injection models and tools
  - Enable the designer to evaluate the circuit early in the design flow
  - Design and Validate new countermeasures against Laser attacks

Utilisation des Techniques Avancées de l'Analyse Statistique dans le Décodage Vidéo Numérique

- Equipe du projet:
  - B. EKOBO A.
  - E. SIMEU
  - F. LEBOWSKY



- Objectif:
  - Améliorer la qualité des vidéos décodées e
  - Respectant la conformité au standard du décodeur (H.264)
  - Assurer une meilleure qualité durant le processus de décodage

Bien vouloir visiter le poster…