DE LA RECHERCHE À L'INDUSTRIE

cea

INSPIRING INNOVATION | INNOVANTE PAR TRADITION

Ecole Nationale Supérieure des Mines SAINT-ETIENNE

Journée sécurité numérique _ GDR SoC-SiP

MISE EN ŒUVRE D'UNE MÉTHODE DE DÉTECTION DE « TROJANS » MATÉRIELS SUR CIRCUITS AES.

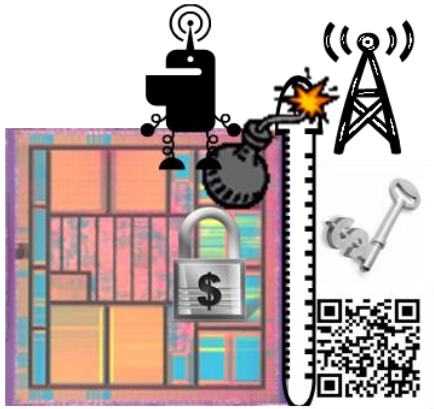
Exurville Ingrid

Jacques Fournier & Jean Max Dutertre

27/11/2012

SOMMAIRE

- Introduction
- Méthode de caractérisation d'un Cheval de Troie Matériel par mesure de temps de chemin de propagation
- Mesure des temps de chemin de propagation sur l'AES
- Mise en œuvre, premières observations
- Perspectives



Introduction

Méthode de caractérisation d'un CTM par mesure de temps de chemin de propagation

Mesure des temps de chemin de propagation sur l'AES

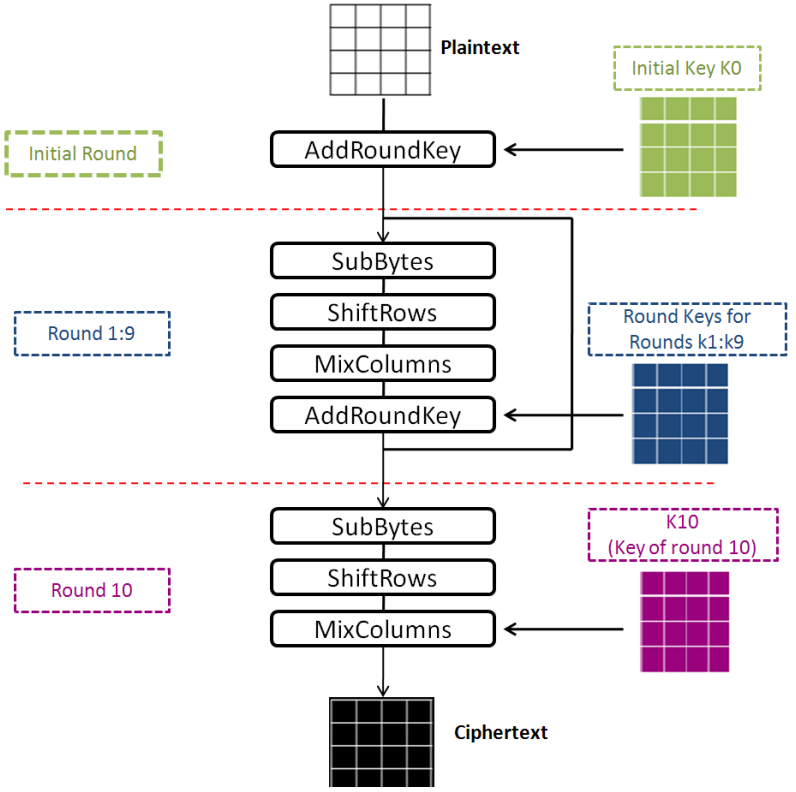
Mise en œuvre, premières observations

Perspectives

Cheval de Troie Matériel

Ajout / modification d'un circuit pouvant transmettre des informations confidentielles à l'insu de l'utilisateur, désactiver/détruire certains composants de la puce…

Approche d'une mesure de temps de chemin de propagation des bits d'un algorithme de chiffrement symétrique par blocs représentés en matrices 4*4 : l'AES.



Hypothèse de travail

L'ajout d'un CTM modifie le temps de propagation des bits.

Introduction

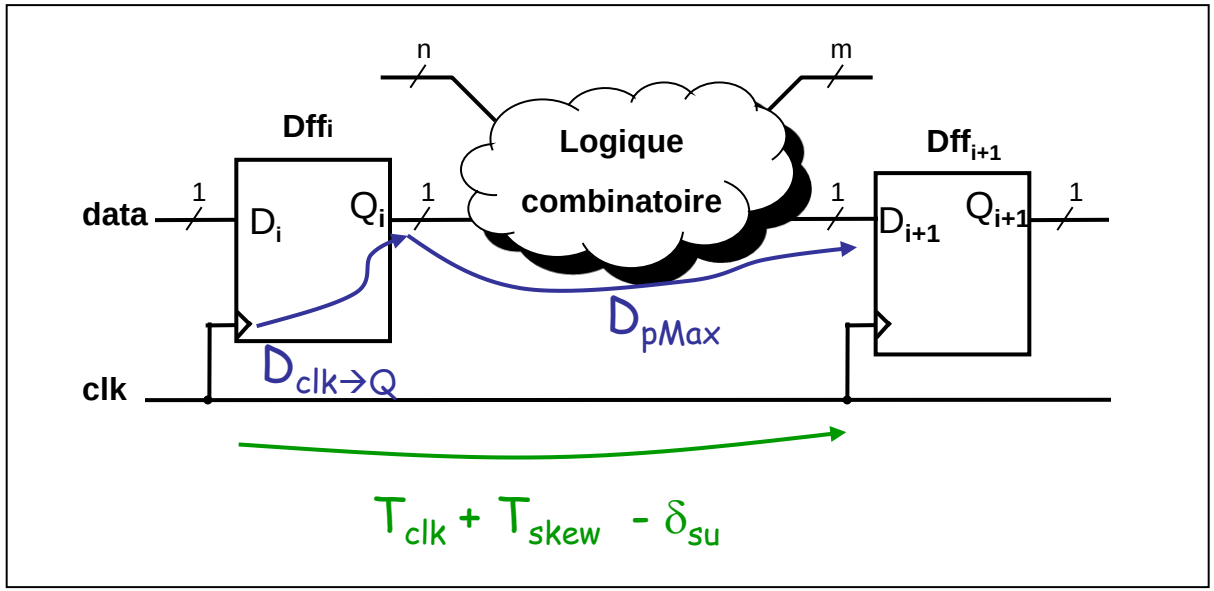
Méthode de Caractérisation d’un CTM par mesure de temps de chemin de propagation

Mesure des temps de chemin de propagation sur l’AES

Mise en œuvre, premières observations

Perspectives

CONTRAINTE TEMPORELLE DES CIRCUITS SYNCHRONES



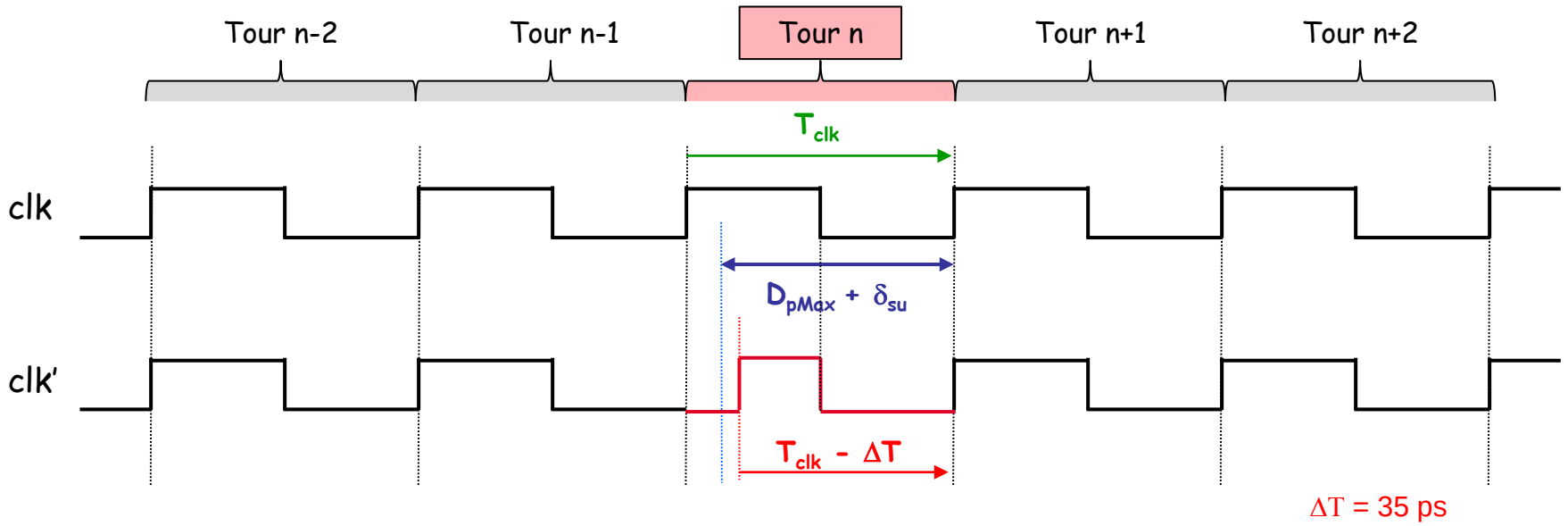
Temps de propagation des données = $D_{clk\rightarrow Q} + D_{pMax}$

Temps requis par les données = $T_{clk} + T_{skew} - \delta_{su}$

$\Rightarrow$ $T_{clk} > D_{clk\rightarrow Q} + D_{pMax} - T_{skew} + \delta_{su}$

LE GLITCH D'HORLOGE

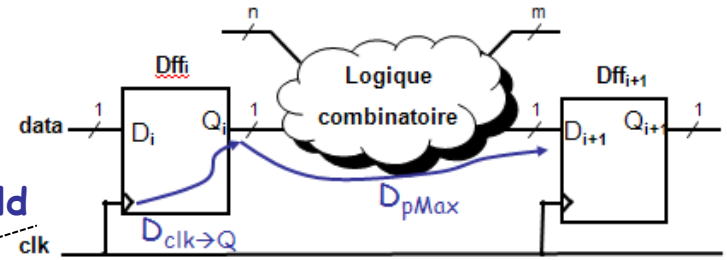
- Le « glitch » d'horloge est une modification locale d'une période.
- Le choix du cycle d'injection est possible.

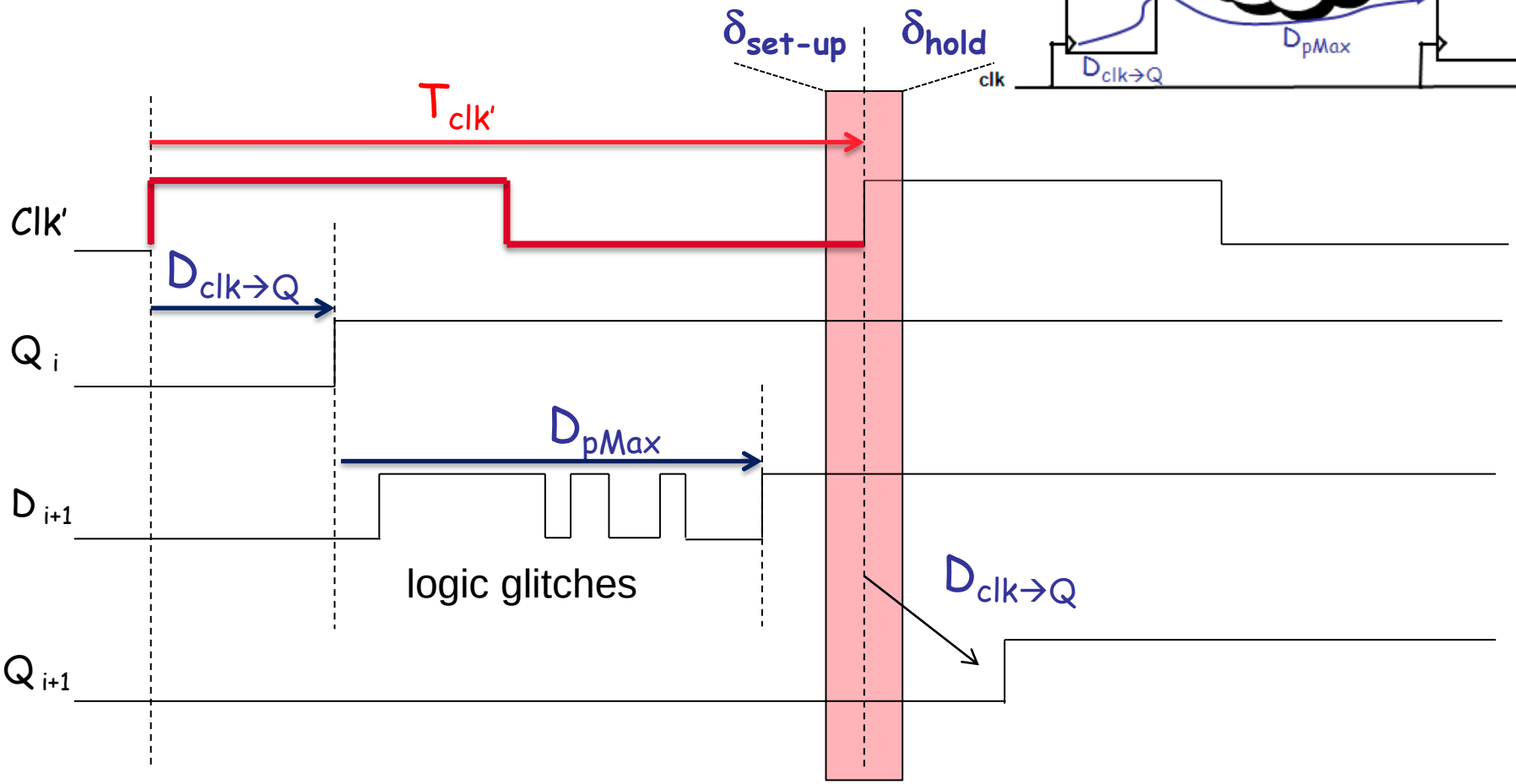


$$T_{clk} > D_{clk \to Q} + \delta_{su} + D_{pMax} - T_{skew}$$

LE GLITCH D'HORLOGE

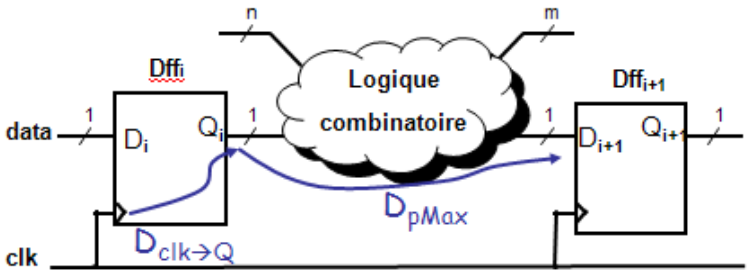
⇒ Fonctionnement normal

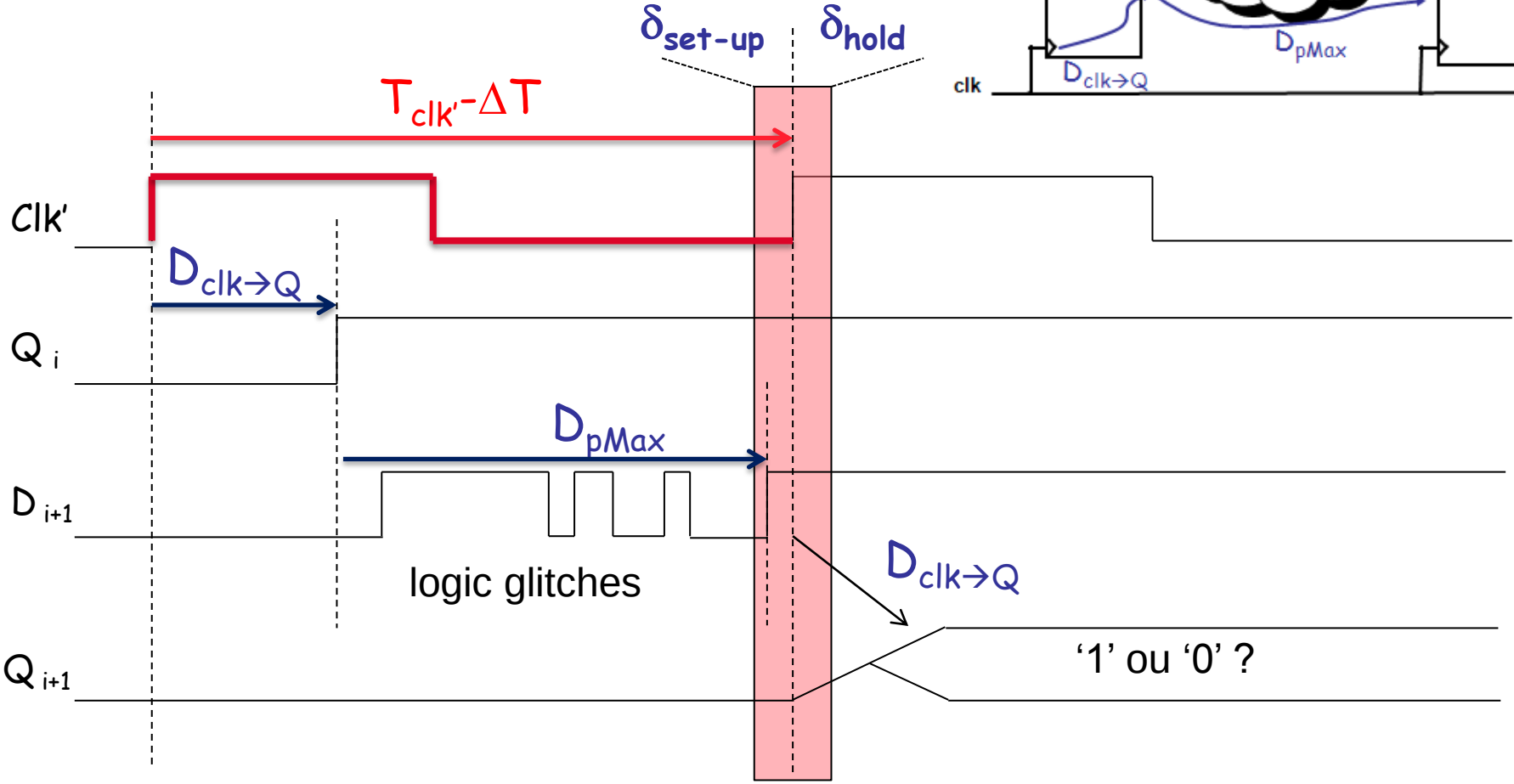




LE GLITCH D'HORLOGE

⇒ Violation du temps de setup

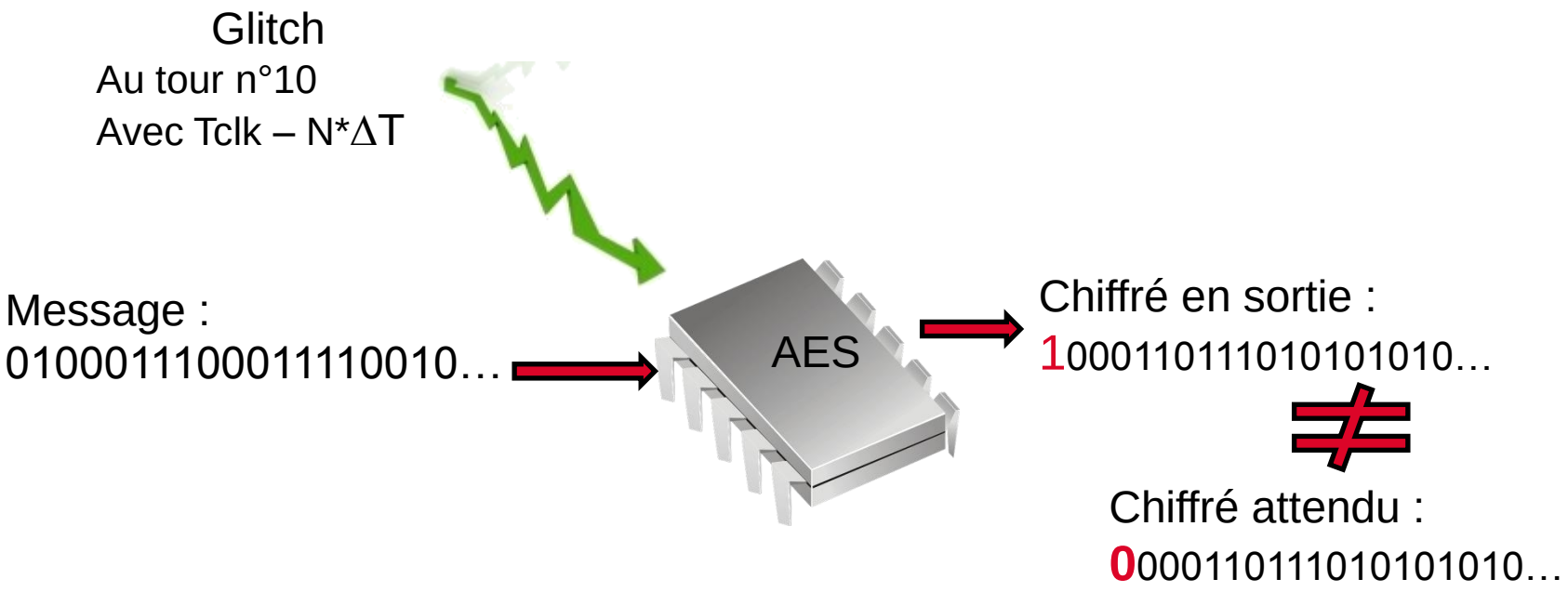




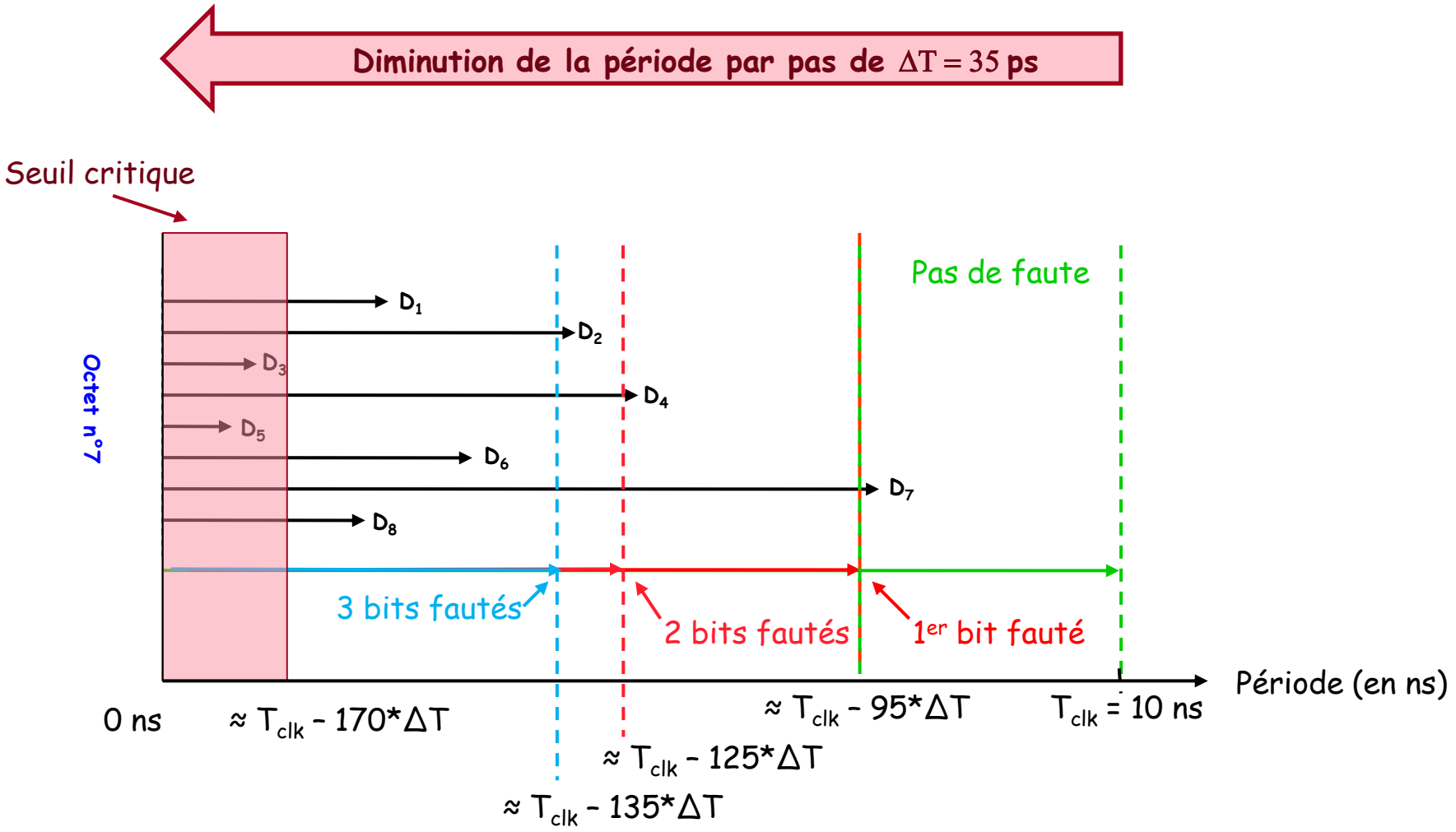
⇒ Métastabilité (non-déterministe)

LE GLITCH D'HORLOGE

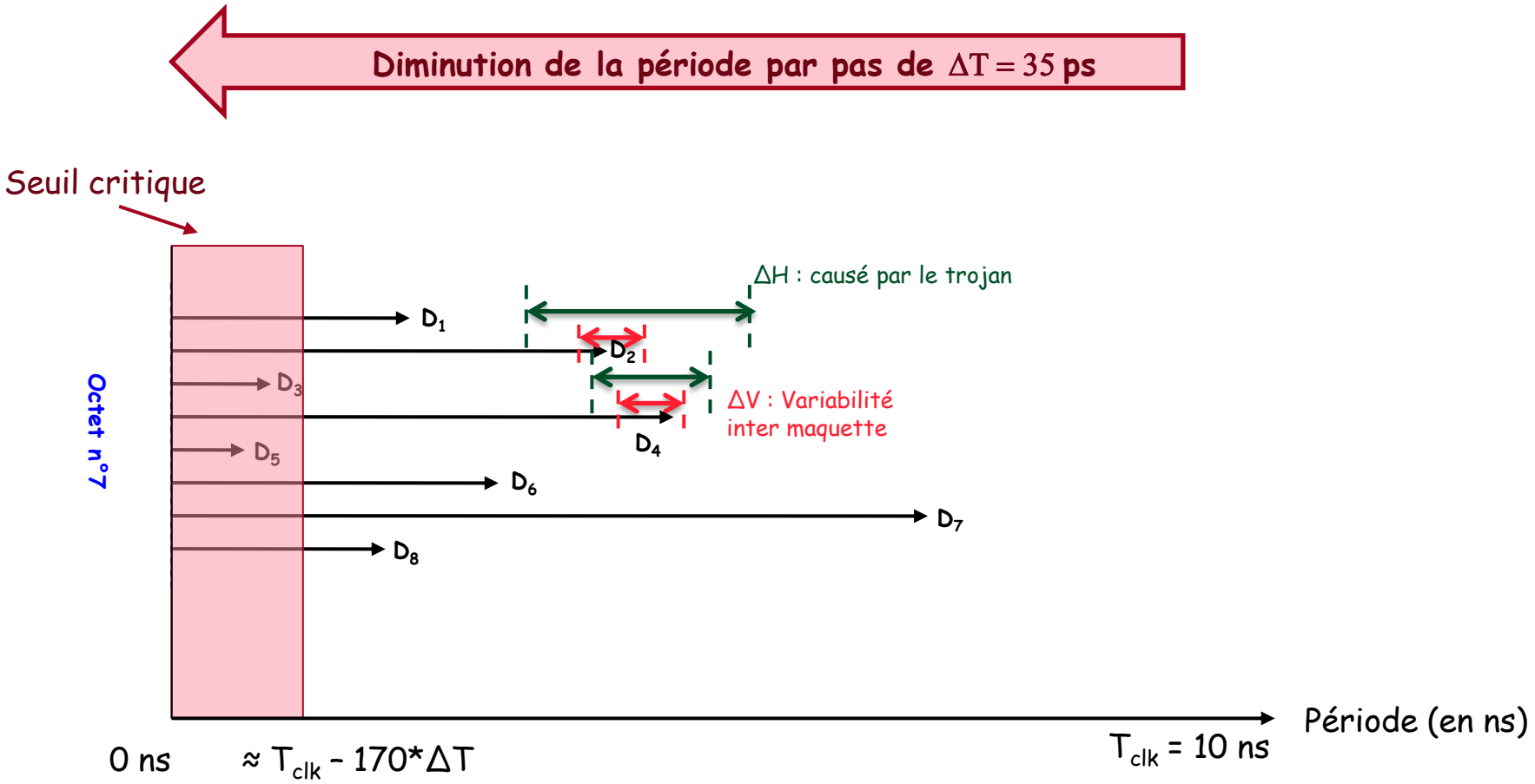
- Faire une faute revient à faire une mesure du temps de propagation des bits connaissant le nombre de ΔT.



PRINCIPE DE DÉTERMINATION DU TEMPS DE PROPAGATION DES BITS



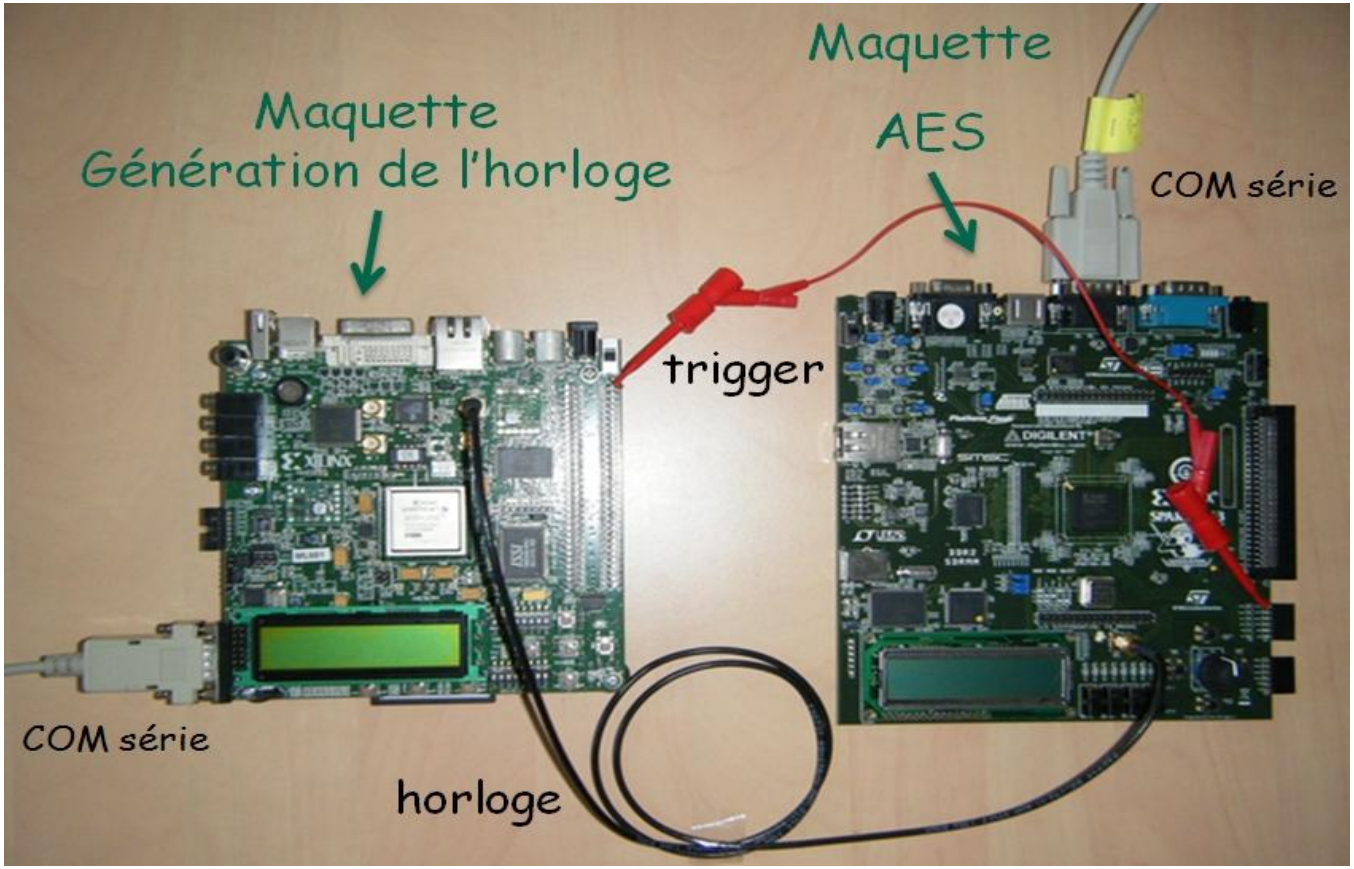
PRINCIPE DE DÉTERMINATION DU TEMPS DE PROPAGATION DES BITS



- Si ΔT << ΔH : on peut mesurer l'effet du CTM.
- Si ΔV << ΔH : La présence du CTM n'est pas masquée par la variabilité.

PROTOCOLE EXPÉRIMENTAL

- Mise en place du glitch d'horloge :



Introduction

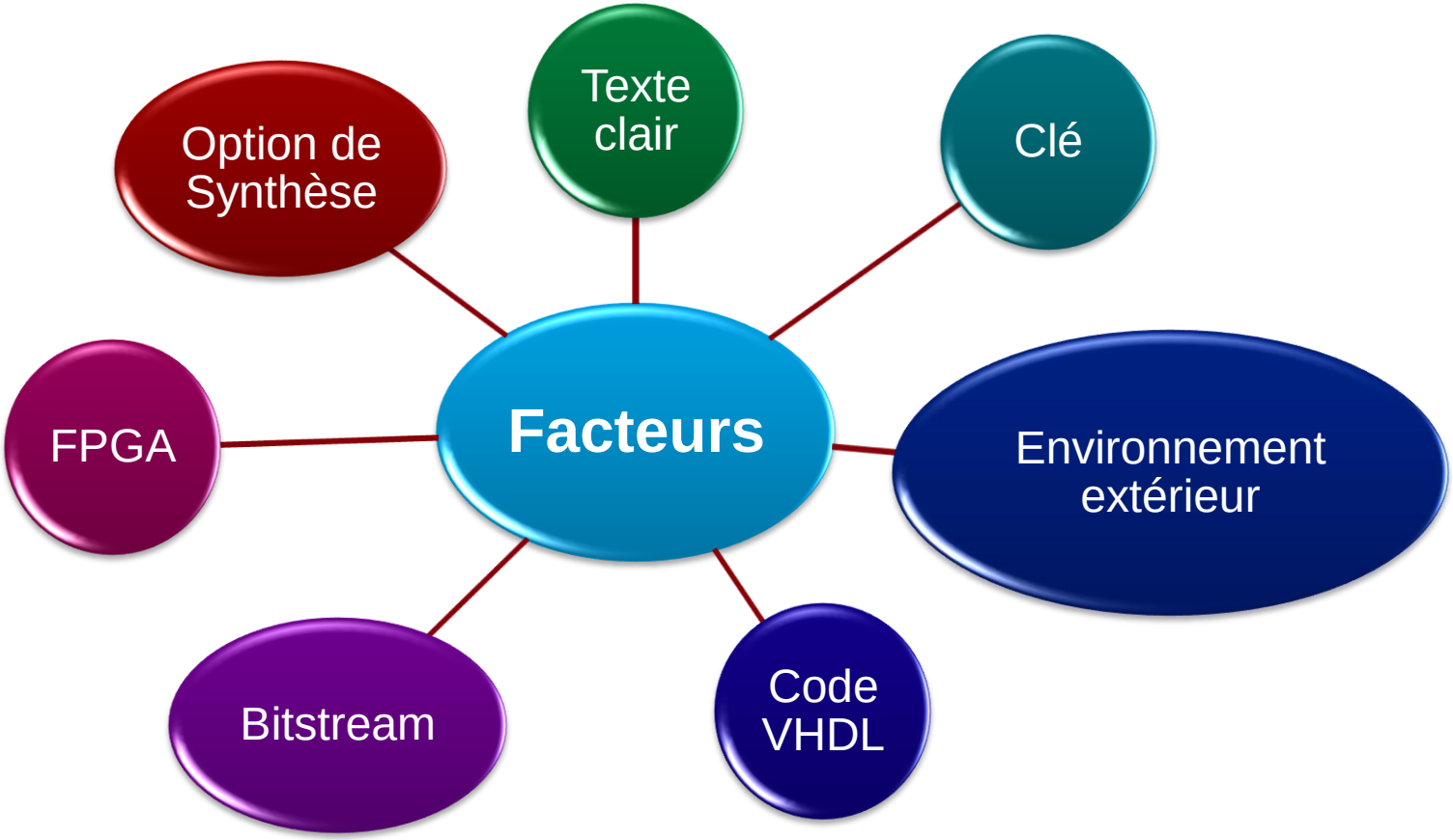
Méthode de caractérisation d'un CTM par mesure de temps de chemin de propagation

Mesure des temps de chemin de propagation sur l'AES

Mise en œuvre, premières observations

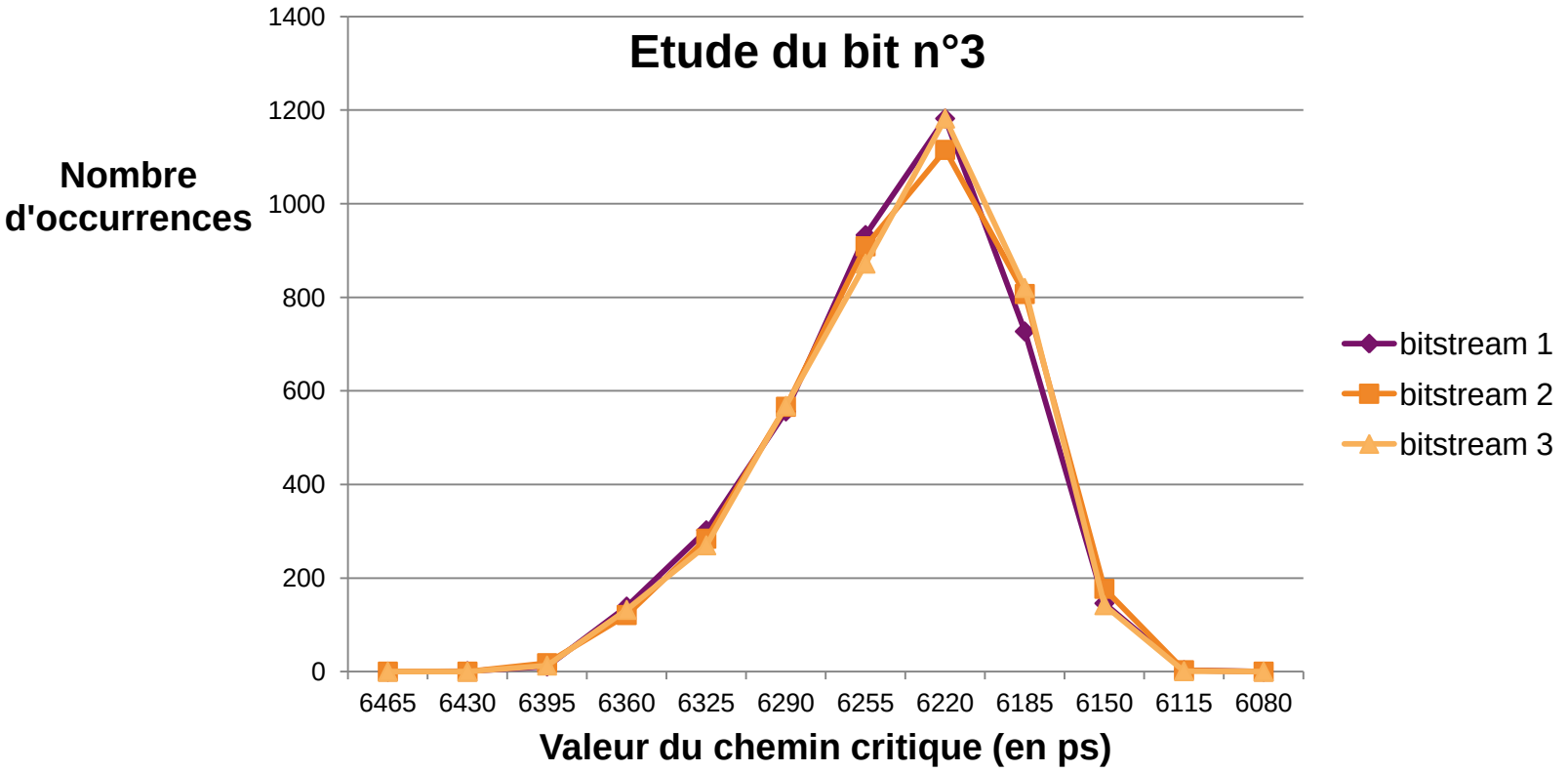
Perspectives

INFLUENCE SUR LA MESURE DES TEMPS DE CHEMINS CRITIQUES SUR L'AES



ETUDE DE LA VARIABILITÉ POUR PLUSIEURS BITSTREAMS SUR UNE MÊME MAQUETTE

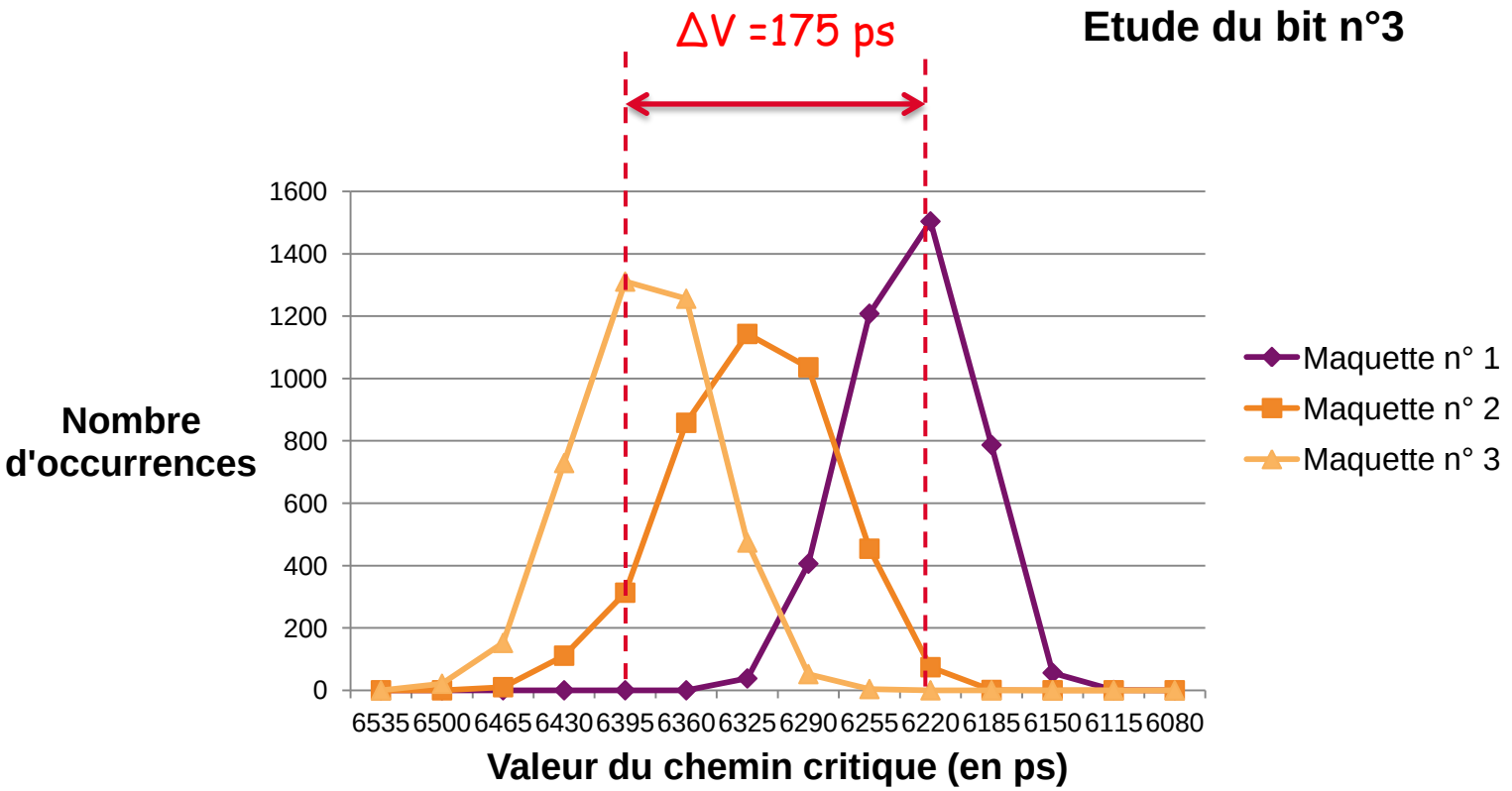
- Trois synthèses distinctes sont effectuées pour en récupérer trois bitstreams.



Texte clair et clé constants

ETUDE DE LA VARIABILITE POUR TROIS MAQUETTES FPGA AVEC UN MEME BITSTREAM

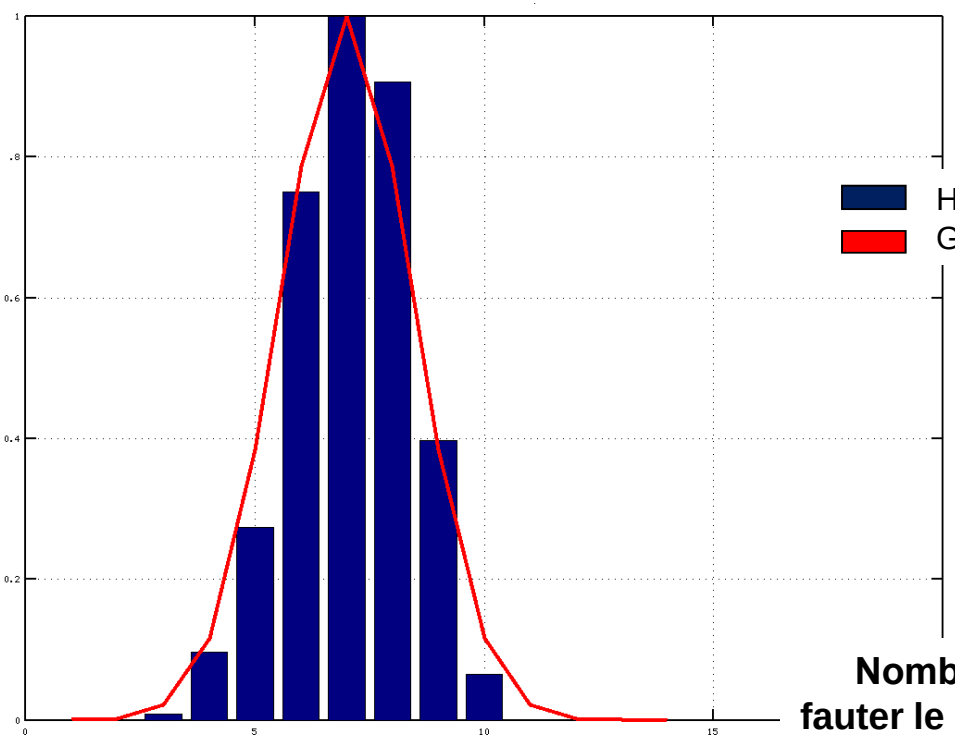
- Même code, même bitstream, trois maquettes
- Texte clair et clé constants.



ETUDE DE LA RÉPARTITION DE TEMPS DE CHEMINS CRITIQUES

- Assimilation à une Gaussienne

Nombre d'occurrences de fautes le bit n°3 pour les 4000 essais

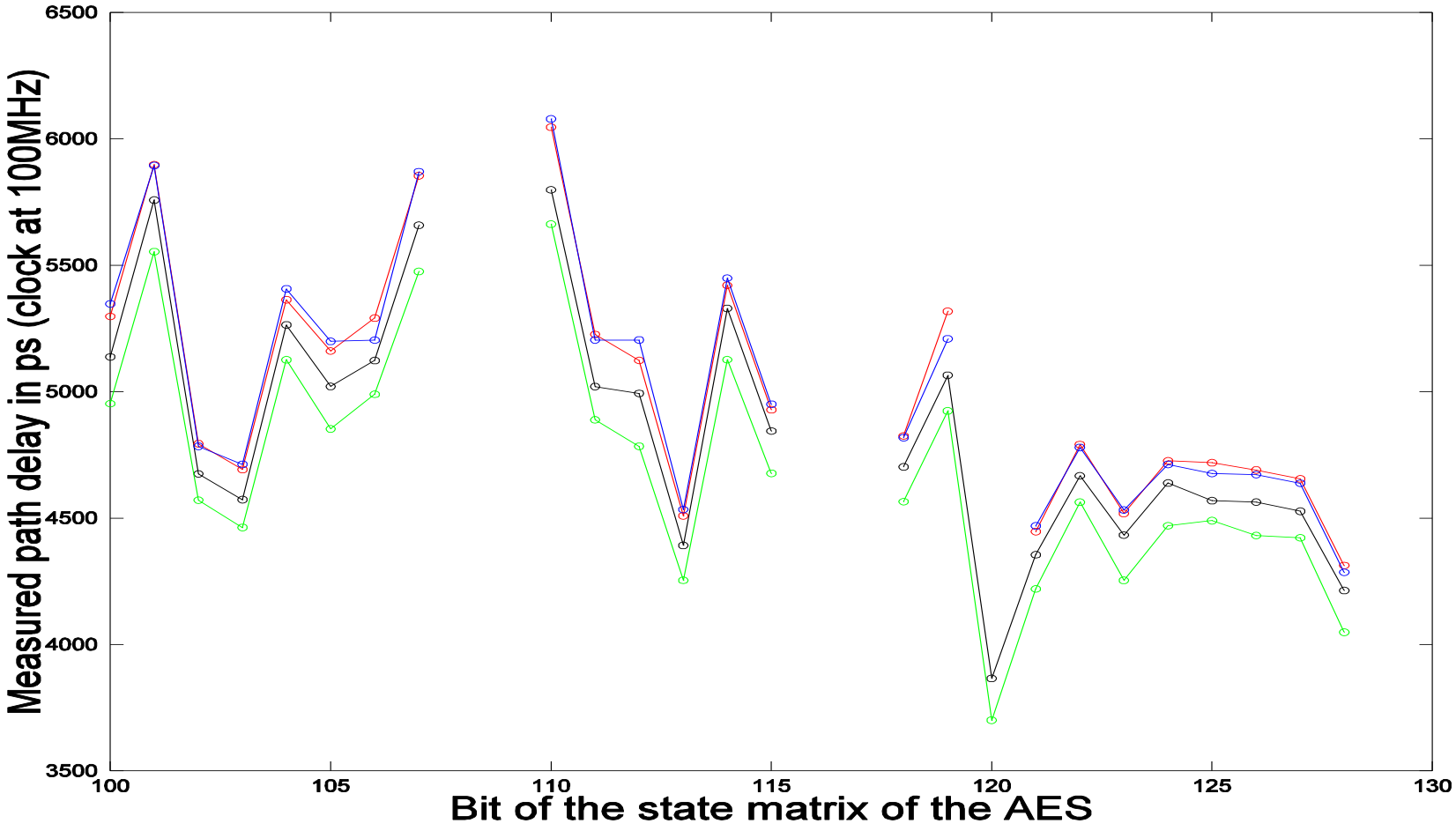


Nombre de ΔT suffisants pour fauter le bit n°3 pour les 4000 essais

Cette méthode permet une certaine formalisation de la base de données des valeurs, et ainsi manipuler les données plus facilement.

ETUDE DE LA VARIABILITE POUR QUATRE MAQUETTES FPGA AVEC UN MEME BITSTREAM

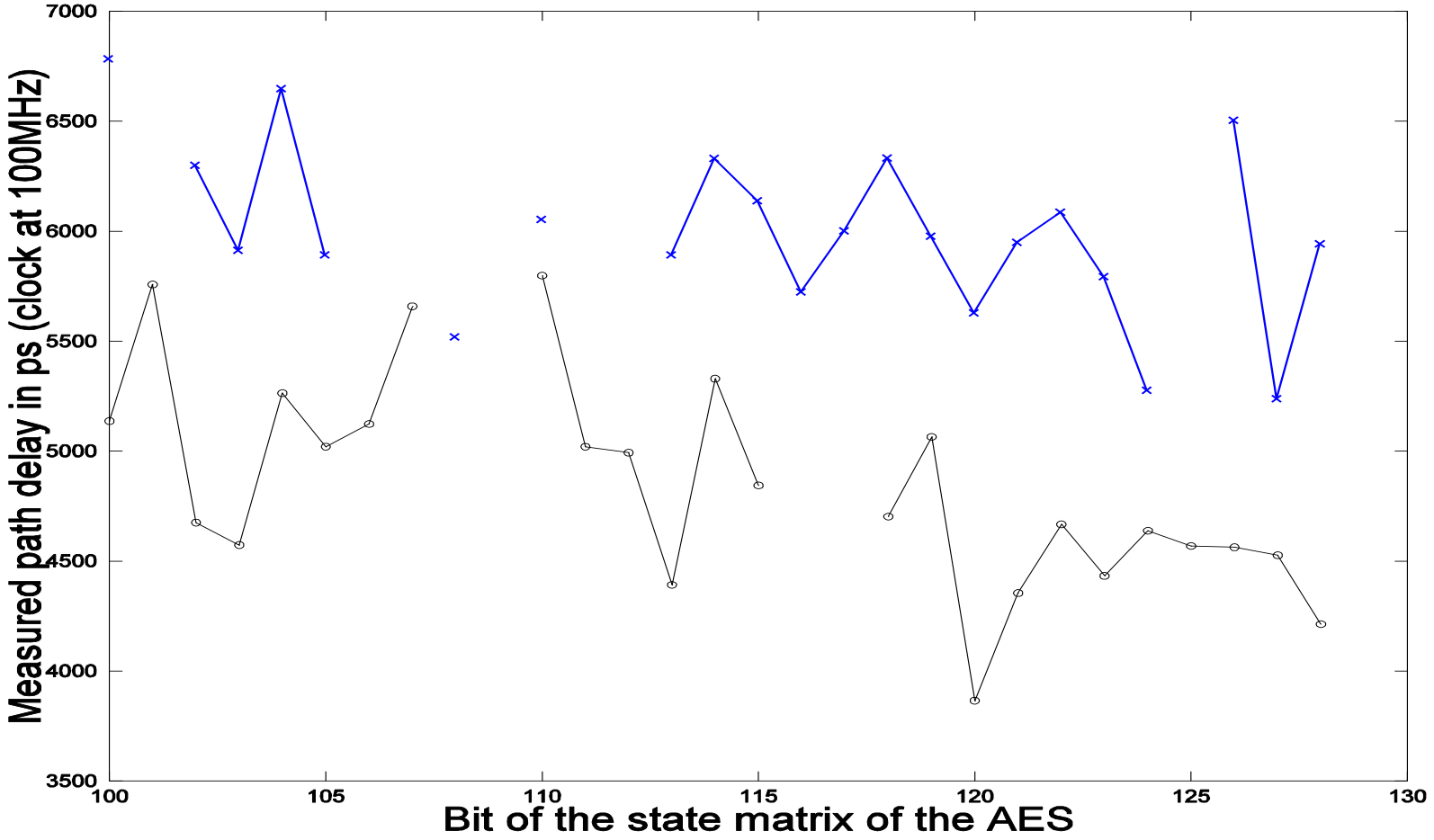
Comparaison des temps de propagation pour quatre maquettes pour les bits [100-128]



OPTION DE SYNTHÈSE « KEEP HIERARCHY »

Comparaison option de synthèse « Keep hierarchy » pour les bits [100-128]

(En noir : sans « Keep hierarchy » , en bleu : avec « Keep hierarchy »)



Introduction

Caractérisation d’un CTM par mesure de temps de chemin de propagation

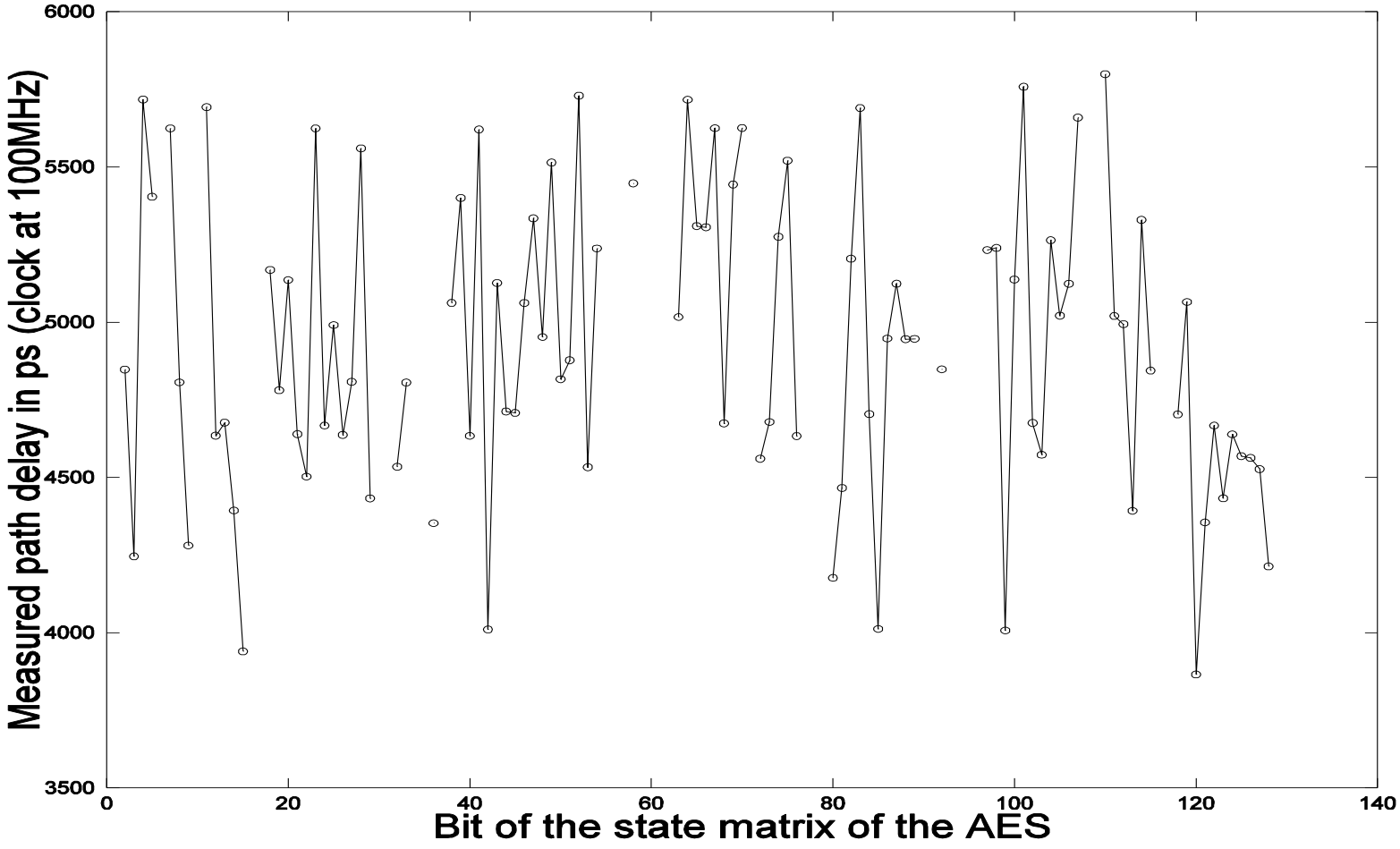
Mesure des temps de chemin de propagation sur l’AES

Mise en œuvre, premières observations

Perspectives

OPTION DE SYNTHÈSE SANS « KEEP HIERARCHY »

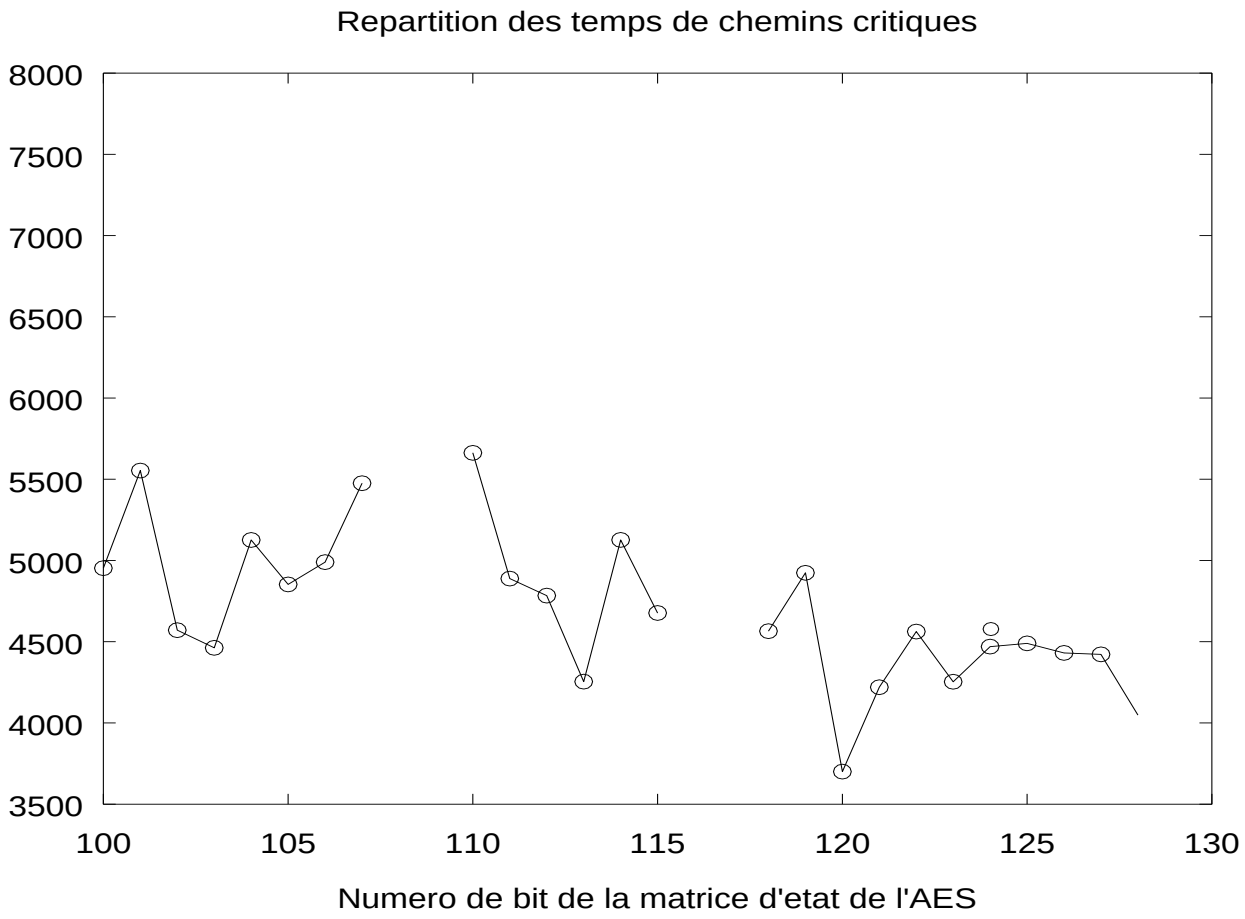
Distribution des temps de propagation des 128 bits de l'AES



OPTION DE SYNTHÈSE SANS « KEEP HIERARCHY »

Comparaison sans CTM/ CTM n°1/ CTM n°2 pour les bits [100-128]

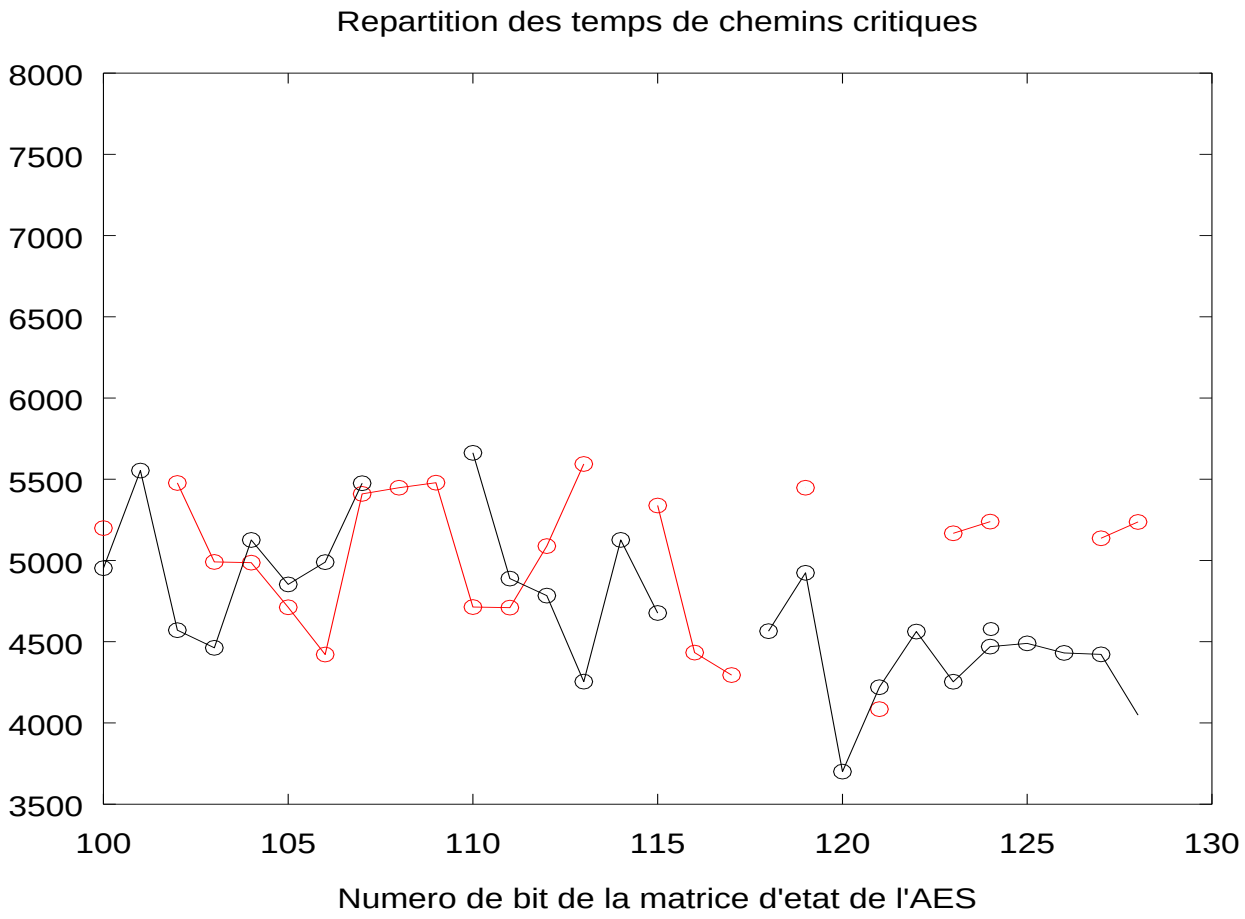
(En noir : sans CTM)



OPTION DE SYNTHÈSE SANS « KEEP HIERARCHY »

Comparaison sans CTM/ CTM n°1/ CTM n°2 pour les bits [100-128]

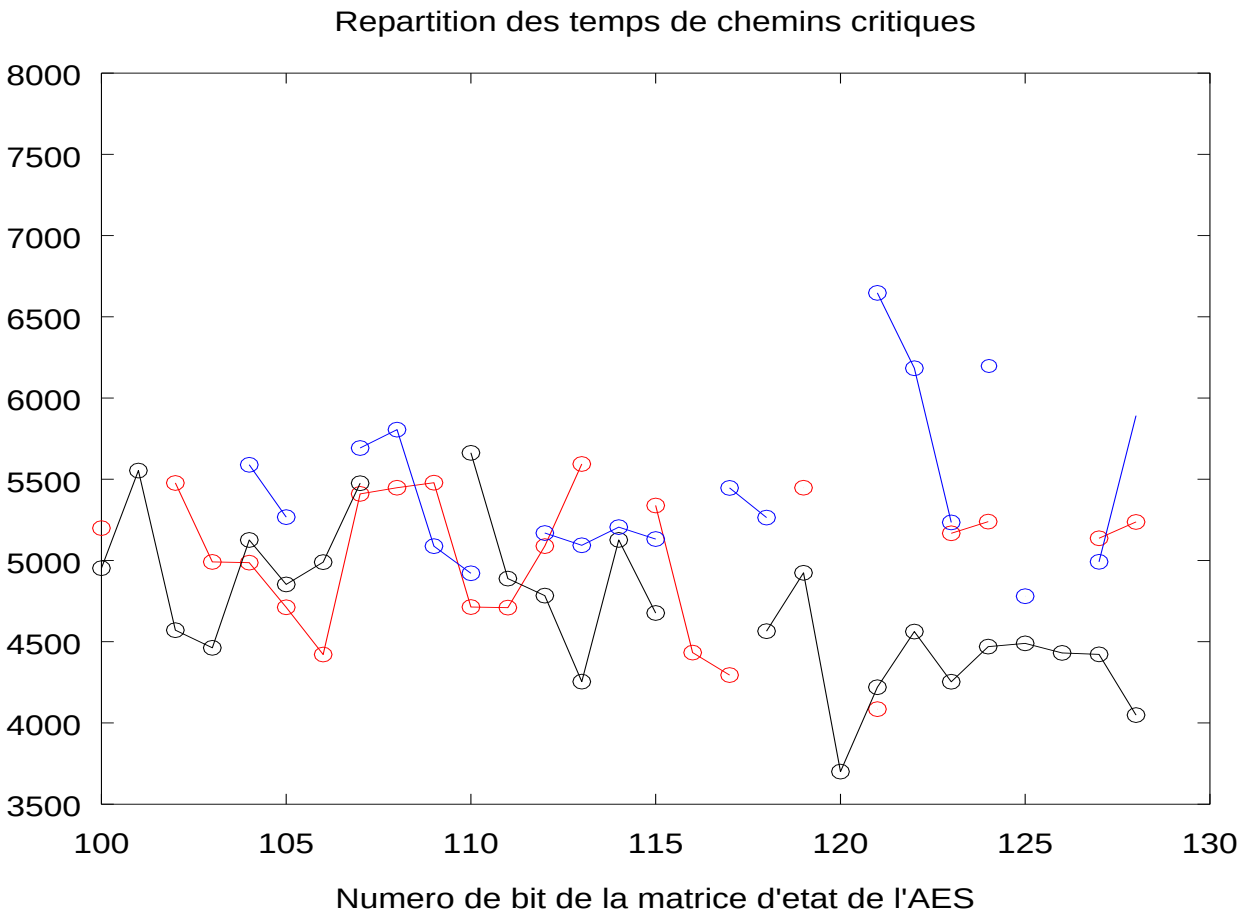
(en noir : sans CTM, en rouge : CTM n°1)



OPTION DE SYNTHÈSE SANS « KEEP HIERARCHY »

Comparaison sans CTM/ CTM n°1/ CTM n°2 pour les bits [100-128]

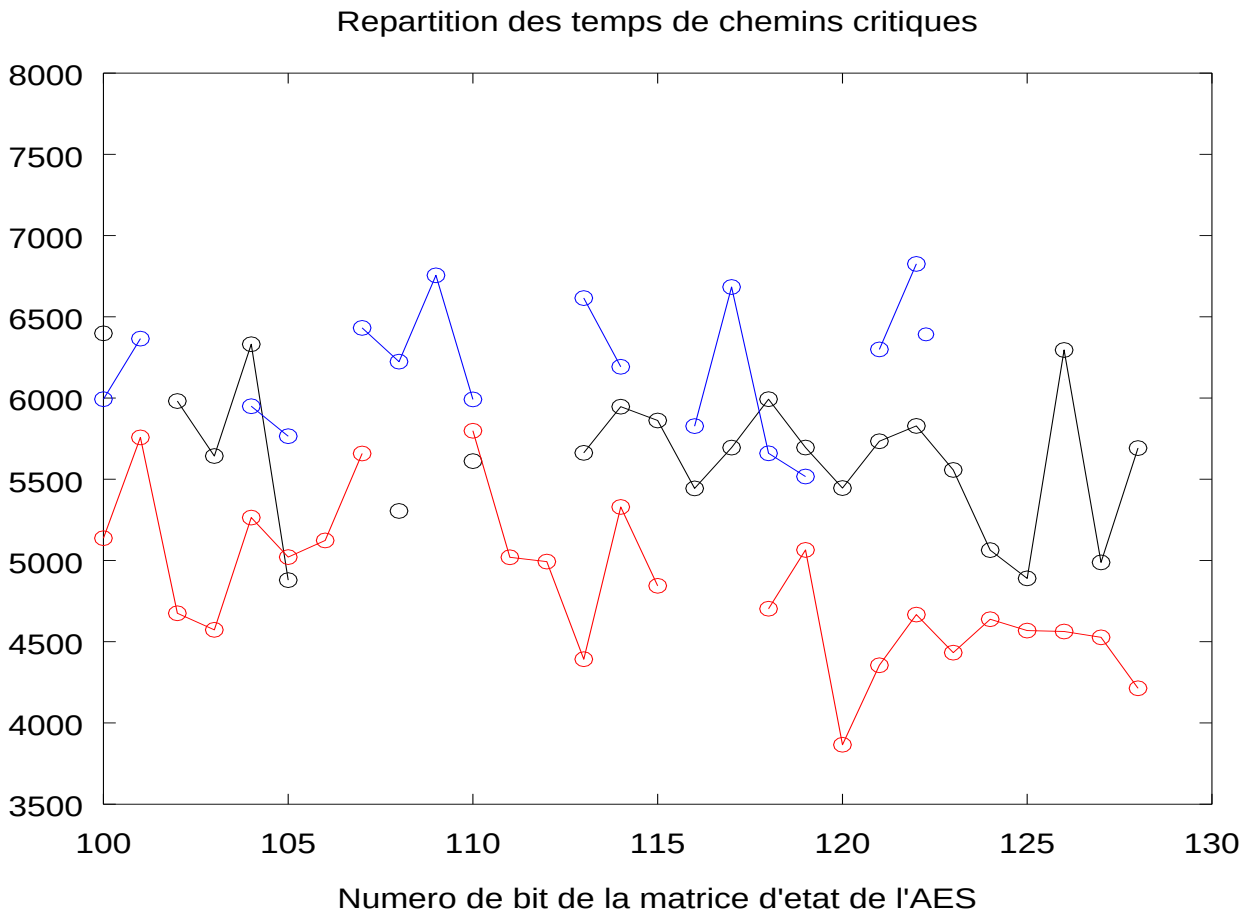
(en noir : sans CTM, en rouge : CTM n°1, en bleu : CTM n°2)



PERTINENCE DE L'OPTION « KEEP HIERARCHY »

Comparaison sans CTM/ CTM n°1/ CTM n°2 pour les bits [60-80]

(en noir : sans CTM, en rouge : CTM n°1, en bleu : CTM n°2)



Introduction

Caractérisation d’un CTM par mesure de temps de chemin de propagation

Mesure des temps de chemin de propagation sur l’AES

Mise en œuvre, premières observations

Perspectives

PERSPECTIVES

- Caractérisation un AES grâce à la distribution des temps associé à chaque bit de l'AES.
- Le rajout d'un CTM a une influence sur la distribution de temps de chemins critiques.
- Les variations dues à certains facteurs (changement de FPGA, d'option, etc.) ont une influence sur le temps de chemins critiques, mais ne remettent pas en cause la validation de l'outil.
- Cette étude a permis de nouvelles approches quant à la détection de CTM.

On distingue des nouveaux critères d'analyses :

  - La liste des bits non détectés
  - L'ordre des bits détectés
  - Le nombre de bits détectés

- Possibilité de détecter une resynthèse.
- Limites : CTM placé dans un chemin « non-critique court ».

Merci pour votre attention

Commissariat à l'énergie atomique et aux énergies alternatives
Centre de Saclay | 91191 Gif-sur-Yvette Cedex

Etablissement public à caractère industriel et commercial | RCS Paris B 775 685 019