

Modélisation des effets de perturbation de la tension d'alimentation sur les circuits CMOS

Anissa Djellid-Ouar^{1,2}, Guy Cathebras¹, Frédéric Bancel²

¹ LIRMM/ UMR5506/ Département MIC
161, rue Ada
34 492 Montpellier Cedex 5

² STMicroelectronics / Division Smartcard
Zone Industrielle de Rousset
13 106 Rousset Cedex

Email : djellid-ouar.lirimm@st.com / djellid@lirimm.fr

Résumé

Plusieurs techniques d'attaques matérielles de circuits sécurisés sont décrites dans la littérature dont les attaques par injection de fautes. Ces dernières consistent à stresser un circuit pour créer un dysfonctionnement temporaire pouvant permettre l'accès à des zones protégées ou à des informations confidentielles. Notre étude a pour but de construire un modèle de fautes DFA (Differential Fault Analysis) liées à la perturbation de la tension d'alimentation d'un circuit CMOS. Ce modèle devra traduire la sensibilité de ce circuit vis-à-vis des perturbations en fonction de la sensibilité des éléments standard qui le composent (logique combinatoire, registres ...). Ce papier présente les travaux de simulations menés à ce jour et leurs résultats.

1. Introduction

Dans le domaine des systèmes sécurisés de type carte à puce, les industriels sont amenés à sans cesse améliorer leurs mécanismes de sécurité tandis que les fraudeurs tentent inlassablement de les déjouer. Cette bataille a conduit à la mise au point de nouvelles techniques d'attaques de moins en moins coûteuses comme la plupart des attaques par injection de fautes. Ce type d'attaque vise à stresser un système pour le faire dysfonctionner.

Le principe de base de toute analyse différentielle telle que la DFA est de trouver une corrélation entre, d'une part, la réponse attendue d'un système, c'est à dire en fonctionnement normal et, d'autre part, sa réponse en état perturbé. Le fait d'amener un circuit à un état de dysfonctionnement temporaire en y injectant des fautes peut donc permettre de remonter à des informations sensées être et rester secrètes, telles que des clés cryptographiques.

Un attaquant peut avoir recours à différents moyens pour injecter des fautes: variations de température, procédés d'irradiations (électromagnétiques, ions lourds...), variations des signaux fournis au circuit à analyser (alimentation, horloge, signal de données...). C'est ce dernier cas auquel nous nous sommes intéressés, et en particulier aux variations transitoires de tension d'alimentation désignées dans la suite de ce document par le terme glitch. Le choix de ce type d'attaque est justifié par le

fait qu'elle soit efficace et facile à mettre en place avec peu de moyens.

Il existe déjà des modèles de fautes décrivant la propagation de transitoires de tension dans les technologies CMOS. Notamment dans le domaine des phénomènes radiatifs et leurs conséquences sur les circuits CMOS. Dans ce domaine précis, les modèles décrivent des événements ponctuels, agissant sur un nœud du circuit étudié. Dans notre cas, nous sommes face à un phénomène global dont les effets touchent le circuit dans sa totalité. Notre travail vise à étudier et à analyser le comportement des cellules standard de la bibliothèque de STMicroelectronics (technologie 0.18 μm) en présence de fautes. En fonction de ce comportement, les chemins les plus sensibles pourront être identifiés. Le modèle DFA devrait ainsi permettre d'anticiper l'effet d'une perturbation (propagation) dans le circuit selon la susceptibilité structurelle des portes qui le constituent, et de l'influence de l'interconnexion de ces portes entre elles.

2. Fautes, erreurs et défaillances

Tout système structuré (biologique naturel ou manufacturé) a tendance à mal fonctionner soit parce qu'il est mal conçu soit parce qu'il se dégrade (environnement). La défaillance d'un système peut se traduire par un dysfonctionnement (temporaire ou permanent) de celui-ci.

Une faute est active lorsqu'elle produit une erreur (instance d'opération incorrecte). Une erreur est en quelque sorte la manifestation d'une faute dans un système. Une erreur conduit à la défaillance (totale ou partielle) d'un système si elle est propagée jusqu'aux sorties du système [1]. Ces mécanismes sont résumés sur la figure 1.

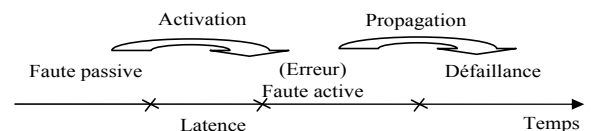


Figure 1 : Manifestation de fautes, erreurs et défaillances

3. Comportement d'une flip flop

On rencontre dans tous les circuits intégrés de nombreuses bascules du type Maître - Esclave comme les D flip flops. Elles sont généralement situées entre deux blocs logiques (cônes logiques). L'objectif ici est d'analyser en simulation le comportement intrinsèque (électrique et logique) d'une flip flop et de la logique qui l'entoure lorsqu'on applique un glitch sur la tension d'alimentation.

3.1 Sensibilité d'une flip flop

Le rôle d'une flip flop est de mémoriser une information le temps nécessaire à son traitement (une période d'horloge). Les valeurs mémorisées forment une image de l'état logique du circuit à un instant donné. Ainsi si l'une de ces valeurs subit une erreur, le circuit passe dans un état logique erroné.

La sensibilité d'une flip flop vis à vis de n'importe quel type de perturbation peut avoir 2 origines [2] :

- les bascules D qui la composent
- la logique qui l'entoure

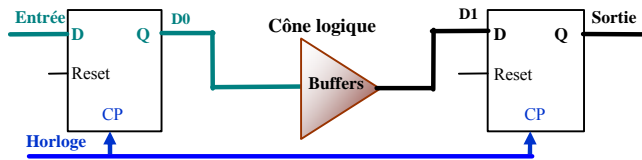


Figure 2 : Flip flop + logique combinatoire

La figure 2 illustre l'un des circuits utilisés en simulation pour l'étude et l'analyse de l'effet d'un glitch sur la tension d'alimentation d'une flip flop.

3.1.1 Simulations

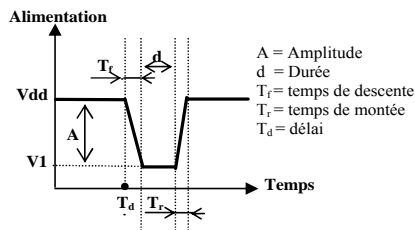


Figure 3 : Modélisation du glitch en tension

La figure 3 est un exemple de représentation électrique d'un glitch (négatif, dans cet exemple, car la tension d'alimentation est abaissée) en simulation avec tous les paramètres qui le caractérisent. Le logiciel utilisé pour nos simulations électriques est ELDO 5.6.

Plusieurs simulations ont été menées afin d'analyser le comportement d'une flip flop standard en présence d'un glitch (négatif ou positif) en faisant varier les paramètres de ce dernier (voir ci-dessus) à chaque simulation. Les résultats obtenus montrent que la fonctionnalité de la flip flop n'est pas altérée. Autrement dit, les bascules D composant la flip flop continuent de fonctionner correctement en dépit de la perturbation de leur tension d'alimentation. La figure 4 représente un exemple de simulation.

Les paramètres de simulation sont les suivants :

- Période d'horloge = $P_{CP} = 6ns$
- Le temps de propagation entre D0 et D1 (chemin le plus long) est de 5ns
- Glitch négatif: $V_{dd} = 1.65V$, $A = 0.65V$, $d = 5ns$ et $T_d = 16ns$

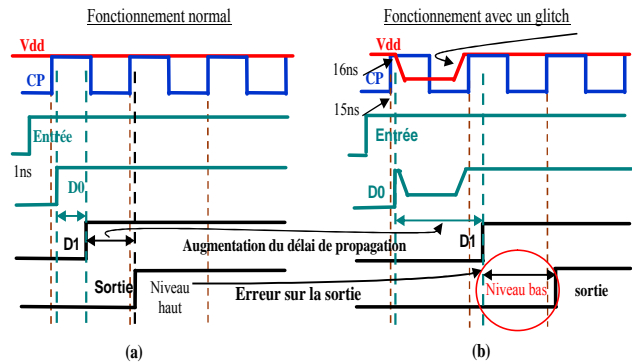


Figure 4 : Simulation d'un glitch négatif sur Vdd

Comme précisé précédemment, la fonctionnalité de la flip flop n'est pas compromise, ceci n'exclue cependant pas l'occurrence d'erreur sur la sortie de la flip flop comme le montre la figure 4 (b). En effet, on observe une erreur sur le signal de sortie au deuxième cycle d'horloge. Cette erreur se manifeste par un bit flip, c'est-à-dire un changement de niveau logique pendant un cycle d'horloge.

L'erreur observée sur le signal de sortie peut s'expliquer de la façon suivante :

- Le glitch négatif appliqué sur Vdd (à $T_d = 16ns$, 1ns après le front actif de CP) a provoqué un ralentissement. Les signaux d'entrée du cône logique, respectivement D0 et D1, sont tous les deux retardés. Le chemin D0 à D1 est le plus long et en fonctionnement normal, le temps de propagation d'un signal à travers ce chemin est $T_p = 5ns$ (avec $P_{cp} = 6ns$)

- Une flip flop échantillonne son entrée afin d'en recopier la valeur à chaque front actif de son horloge. Cette opération ne se fait pas instantanément. Comme le montre la figure 5, certains délais doivent être respectés :

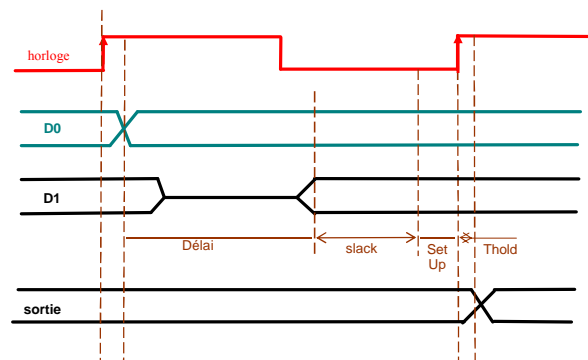


Figure 5 : Chronogramme d'une flip flop

- Délai = temps nécessaire à la transmission du signal de l'entrée à la sortie du buffer
- T_{setup} = temps d'établissement de la donnée à l'entrée de la flip flop avant le front actif de l'horloge
- T_{hold} = temps de maintien de la donnée après le front actif de l'horloge

- Slack (jeu)= temps restant entre le délai et le moment de set up.

Ces conditions réunies font qu'au second front actif de l'horloge, le signal D1 est encore au niveau bas à cause du retard occasionné par le glitch négatif sur Vdd. De ce fait, c'est ce niveau qui est transmis en sortie et non un niveau haut comme cela aurait dû être le cas.

3.1.2 Conclusions

- Une erreur survenant à la sortie d'une flip flop ou d'un registre dont la tension d'alimentation est perturbée par un glitch, n'est pas attribuable à la flip flop elle-même. En effet, la fonctionnalité de cette dernière n'est pas altérée en présence du glitch. Par conséquent, suite aux différentes simulations que nous avons effectuées, les bascules D constituant une flip flop, semblent résistantes aux glitches sur leur tension d'alimentation.

- Ce premier résultat est non sans importance. Cela revient à dire que la perturbation de la tension d'alimentation provoque des violations de délai. Ceci nous amène à nous focaliser sur le comportement de la logique combinatoire entourant une flip flop en présence d'un glitch. Le terme « logique » inclut aussi l'arbre d'horloge.

4. Perspectives : Comportement de la logique combinatoire

Cette partie est toujours en cours d'étude. Notre but est de dégager des critères de sensibilité aux fautes d'une flip flop ou d'un registre, sensibilité désormais liée, comme mentionné dans la section 3.1.2, au comportement de la logique combinatoire.

Notre objectif est donc d'étudier la propagation d'une perturbation de tension dans la logique combinatoire. Nous effectuons cette étude sur des circuits simples assurant la même fonction, mais de structure différente (longueur, chemins reconvergeants...) comme le montre l'exemple de la figure 6.

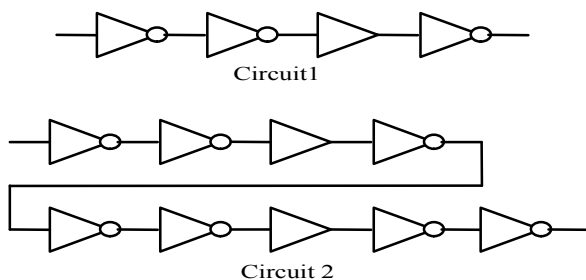


Figure 6 : Exemple de cônes logiques

Le but est de différencier l'effet d'une perturbation sous différentes conditions :

- longueur du cône
- type de glitch : positif ou négatif
- taille du glitch : amplitude et durée
- niveau logique au moment de la perturbation
- étude statique et dynamique
- ...

Les conclusions de cette partie nous permettront de définir les structures de cônes les plus sensibles. Ces résultats seront utilisés pour deux axes :

- Affectation d'un critère de sensibilité à une flip flop (relatif à son cône logique) pour des simulations d'injection de fautes au niveau logique
- Contre mesure : définition de règles de conception pour éviter les structures de cônes sensibles

Références

- [1] L. Anghel. *Test des circuits intégrés*. ENSERG-INP Grenoble. Cours de l'école d'électronique numérique IN2P3, 2003.
- [2] J.M.Dutertre. *Circuits reconfigurables robustes*. Thèse de doctorat, Université Montpellier 2, LIRMM, Octobre 2002