DESIGN AND SECURITY EVALUATION OF SECURE CRYPTOHARDWARE (FPGA AND ASIC) AGAINST HACKERS EXPLOITING SIDE-CHANNEL INFORMATION

(DISEÑO Y EVALUACIÓN DE LA SEGURIDAD DE HARDWARE CRIPTOGRÁFICO SEGURO (FPGA Y ASIC) FRENTE A HACKERS QUE EXPLOTAN INFORMACIÓN DE CANAL LATERAL)

Erica Tena-Sánchez[1], F. Eugenio Potestad-Ordóñez[1], Pilar Parra- Fernández[1], Carmen Baena-Oliva[1], Manuel Valencia-Barrero[1], Carlos Jesús Jiménez-Fernández[1] y Antonio J. Acosta-Jiménez[2]

[1]Departamento de Tecnología Electrónica, Universidad de Sevilla, Sevilla
[2]Departamento de Electrónica y Electromagnetismo, Universidad de Sevilla, Sevilla
E-mail de correspondencia: etena@us.es

RESUMEN

Tradicionalmente, la seguridad en los dispositivos criptográficos estaba ligada exclusivamente a la fortaleza del algoritmo. El nivel de seguridad venía determinado por la formulación matemática y la longitud de la clave. Sin embargo, la implementación física de los circuitos criptográficos tiene fugas de información como pueden ser el consumo de potencia o la radiación electromagnética, que puede ser explotadas por potenciales hackers para revelar la clave secreta. Uno de los ataques más potentes es el que se basa en análisis del consumo de potencia, conocido como *Differential Power Analysis (DPA) attack*. El DPA utiliza la dependencia del consumo de potencia con los datos procesados para revelar información. Para proteger los circuitos criptográficos se utilizan ampliamente estilos de lógica diferencial con un consumo de potencia (casi) constante. En este trabajo se proponen diferentes metodologías de diseño de celdas diferenciales mediante la redistribución de la carga almacenada en los nodos internos, eliminando el efecto memoria que aparece como un agujero importante en la seguridad. Las celdas propuestas eliminan la carga residual en el circuito y simplifican la estructura de la celda. Para demostrar la ganancia en prestaciones, se han diseñado, implementado físicamente y caracterizado experimentalmente estas celdas en la tecnología de TSMC de 90nm. Los resultados experimentales muestran una reducción del 15% en el área, del 11% en el consumo de potencia y sin degradación en el retraso de las puertas propuestas. Para demostrar la mejora en seguridad, se han desarrollado ataques DPA basados en simulación.

1. INTRODUCCIÓN

Los *Differential Power Analysis (DPA) attacks* han sido ampliamente utilizados debido a su simplicidad y efectividad [1] para obtener la clave secreta mediante la observación del consumo de potencia consumida durante la encriptación. Por esta razón, la comunidad científica ha mostrado un especial interés en diseñar contramedidas contra los ataques DPA, haciendo que todo el sistema sea seguro contra este tipo de ataques. En la Figura 1 se muestra una clasificación de las contramedidas propuestas contra el DPA.

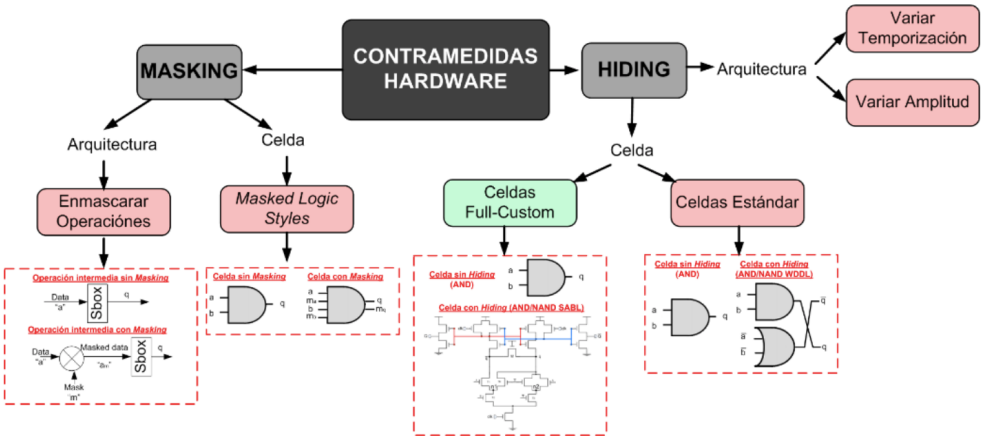

Figura 1. Contramedidas hardware frente a DPAs.
Fuente: elaboración propia.

2. CONTRAMEDIDAS FRENTE A DPA

Existen varias contramedidas aplicables a diferentes niveles de abstracción, desde el nivel de arquitectura o algoritmo a nivel de celda. A nivel de celda, las contramedidas pueden clasificarse en dos categorías: *masking* (enmascaramiento) y *hiding* (ocultación). El masking trata de aleatorizar los valores intermedios procesados por el dispositivo criptográfico durante el cifrado. Básicamente, cada valor intermedio se enmascara con un valor aleatorio *m* llamado máscara, siendo a_m = a xor *m*. Sin embargo, se ha demostrado que los estilos de lógica basados en *maskig* sólo aumentan ligeramente el número de patrones necesarios para lograr un ataque exitoso. Por otro lado, las técnicas de *hiding* a nivel de celda intentan tener el mismo consumo de energía independientemente de los datos que se procesan. Las técnicas de *hiding* que ofrecen los mejores resultados contra los ataques DPA son las que se basan en la lógica ***Dual-Precharge Logic.***

3. PROPUESTA

Para implementar celdas de bajo consumo para aplicaciones criptográficas seguras (priorizando los niveles de seguridad), este trabajo toma como vehículo de demostración la celda XOR/XNOR. En las celdas *Sense Amplifier Based Logic* (SABL [2], ver estructura en la Figura 2a), que utilizamos como referencia por su amplia aceptación en la comunidad científica como estructura segura, se puede apreciar una brecha de seguridad. En los nodos internos n1 y n2 del pull-down de la celda, se pueden observar niveles de voltaje diferentes que pueden ser explotados mediante ataques DPA (ver Figura 2b).

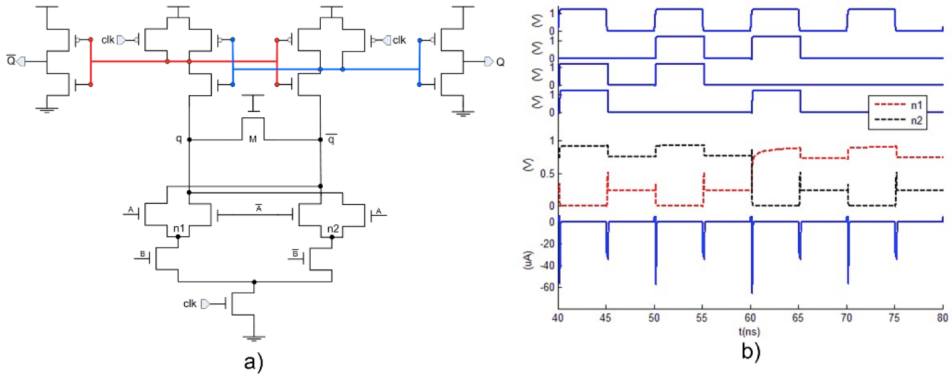

Figura 2. Estructura celda SABL y simulación eléctrica de los nodos internos.
Fuente: elaboración propia.

Para recudir el consumo y no degradar la frecuencia de operación máxima de las celdas se propone utilizar en el pull-up la estructura DDCVSL. Para eliminar el efecto memoria, proponemos la inclusión de la contramedida *dual-switch* que consiste en añadir dos transistores P en los nodos n1 y n2 del pull-down igualando el voltaje en estos nodos en fase de precarga (ver Figura 3).

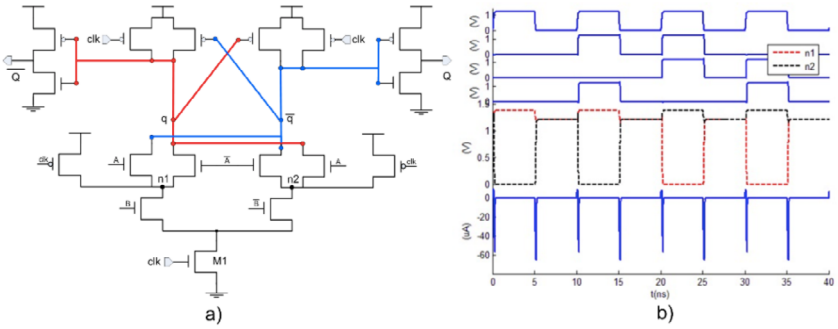

Figura 3. Estructura propuesta y simulación eléctrica de los nodos internos.
Fuente: elaboración propia.

4. RESULTADOS Y CONCLUSIONES

Con la estructura propuesta, conseguimos reducir el consumo de potencia en un 11%, un 15% en área y sin degradación en la frecuencia de operación. Por otra parte, tras realizar ataques DPA sobre las nuevas implementaciones, hemos podido observar una mejora en seguridad por encima de x50.

Tabla 1. Resultados Experimentales.

RESULTADOS EXPERIMENTALES			
	SABL	**Propuesta**	**% de mejora**
Área (μm²)	33.72	28.46	15.60 %
Delay	6.04	5.90	2.32 %
Power	600.00	532.80	11.20 %
Security (MTD)	200	>>10000	>>5000%

Fuente: elaboración propia.

AGRADECIMIENTOS

Este trabajo ha sido financiado por el proyecto de I+D+i PID2020-116664RB-I00, financiado por MCIN/ AEI/10.13039/501100011033, por el Programa Operativo FEDER 2014-2020 y Consejería de Economía, Conocimiento, Empresas y Universidad de la Junta de Andalucía bajo el proyecto US- 1380823 y por SPIRS (Secure Platform for ICT Systems Rooted at the Silicon Manfacturing Process) Project with Grant Agreement No. 952622 under the European Union's Horizon 2020 research and innovation programme.

REFERENCIAS BIBLIOGRÁFICAS

Kocher, P., Jaffe, J., & Jun, B. (1999). Differential Power Analysis, *CRYPTO Conference*, 388-397. doi: https://doi.org/10.1007/3-540-48405-1_25

Tiri, K., Akmal, M., & Verbauwhede, I. (2002). A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on Smart Cards, ESSCIRC Conference, 403-406.