PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

DISEÑO DE CIRCUITO DE PROTECCIÓN CONTRA EXTRACCIÓN DE INFORMACIÓN SECRETA EN TARJETAS INTELIGENTES

Tesis para optar el Título de **Ingeniero Electrónico,** que presenta el bachiller:

Guillermo Gabriel Garayar Leyva

ASESOR: MSc. Julio César Saldaña Pumarica

Lima, febrero de 2014

RESUMEN

En el presente trabajo de tesis se realizó el diseño de un circuito de protección contra ataques del tipo *Differential Power Analysis* (DPA) aplicado a tarjetas inteligentes. Este tipo de tarjetas presenta la misma apariencia física de una tarjeta de crédito pero en su estructura cuenta con un circuito integrado.

Se utilizó la tecnología AMS 0.35 μm de la compañía Austriamicrosystem, y se aplicó la técnica denominada Atenuación de Corriente. Esta se basa en la implementación de un circuito ubicado entre la fuente de alimentación y el procesador criptográfico de la tarjeta inteligente, el cual logra disminuir las variaciones de consumo de corriente presentes durante una operación criptográfica.

El circuito de protección se dividió en tres bloques: Sensor de Corriente, Amplificador de Transimpedancia e Inyector de Corriente. Cada uno de estos bloques fue diseñado tomando criterios del diseño de circuitos integrados analógicos, tales como consumo de potencia, área ocupada y ganancia. Para esta etapa de diseño se utilizó el modelo *Level 1* del transistor MOSFET.

Posteriormente, se realizaron simulaciones a cada uno de los bloques del circuito de protección usando el software Cadence. Finalmente, una vez alcanzados los requerimientos establecidos, se procedió al desarrollo del *layout* físico del circuito diseñado.

El circuito diseñado logra una atenuación de las variaciones de consumo de corriente del 86%. Entre sus principales características se puede mencionar que consume $35.5mW$, ocupa $60000\mu m^2$ y presenta $96MHz$ de ancho de banda.

A mis padres Guillermo y Gabriela, por su amor incondicional.
A mi hermano Alejandro, por su alegría y cariño.
A mis abuelos Esteban, María, Benjamín, Yolanda, Carmen y Jacinto, por su gran ejemplo y motivación.
A mis asesores Julio y Erick, por su confianza y todas las enseñanzas brindadas.
A Sammy, Edward, Eduardo, Niels, Coco, Andrés, Renato, Mónica, Tamara, Edith, Michael, Cubo, Héctor, Alejo, André, Ronald, Carlos, Stefano, Álvaro, Christian y todos mis amigos, por su gran ayuda y amistad.

!Muchas gracias a todos!

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El uso de tarjetas inteligentes se ha extendido alrededor del mundo debido a su viabilidad y portabilidad [1]. Estas pueden ser utilizadas para almacenar firmas digitales, documentos confidenciales, dinero electrónico, etc. Una de las principales características de estas tarjetas es la seguridad que ofrece debido a los algoritmos criptográficos que utiliza, tales como el *Data Encryption Standard* (DES) [12]. Sin embargo, el acceso a la información contenida en la tarjeta inteligente puede realizarse por medio de la medición de la corriente consumida por la misma.

Existen técnicas que utilizan el consumo de potencia para obtener información contenida en tarjetas inteligentes, pero la más agresiva y difundida es conocida como *Differential Power Analysis* (DPA), la cual realiza un análisis estadístico a la señal de corriente consumida de la tarjeta inteligente [6].

Este riesgo ha creado la necesidad de incrementar la seguridad de la información de los usuarios. Por este motivo se han planteado soluciones que implican el uso del diseño analógico de circuitos integrados [7], [8], [9], [10]. Estas toman en cuenta criterios puntuales como consumo de potencia, área ocupada y ganancia.

En el presente trabajo, se busca diseñar un circuito en tecnología CMOS, que sea capaz de proteger a tarjetas inteligentes frente ataques del tipo DPA. Los criterios para medir la eficiencia del circuito de protección serán el porcentaje de atenuación de variaciones de consumo de corriente y el ancho de banda del mismo.

El presente documento se divide en cuatro capítulos. En el primer capítulo, se presentan los tipos de ataques que sufren las tarjetas inteligentes, así como las soluciones que existen para combatirlos. En el segundo capítulo, se muestra la teoría sobre la tecnología CMOS y se define la topología a usar. Luego, en el tercer capítulo se muestra el diseño del circuito de protección. Finalmente, en el cuarto capítulo se muestran las simulaciones y los resultados obtenidos.

CAPÍTULO 1

ATAQUES DPA Y LA MICROELECTRÓNICA

1.1 INTRODUCCIÓN

En la actualidad, el uso de tarjetas inteligentes está muy difundido debido a la facilidad que otorgan al usuario para llevar información confidencial. Estas pueden ser utilizadas para almacenar firmas digitales, dinero electrónico, historial clínico, contraseñas, etc. Sin embargo, existen técnicas para extraer esta información ya que este tipo de tarjetas es vulnerable ante el análisis de la disipación de potencia, temporización o la radiación electromagnética que presentan durante la ejecución de una operación [6].

Las técnicas más difundidas para quebrar la seguridad de las tarjetas inteligentes se basan en la potencia consumida por estas. Estas se pueden clasificar en: *Simple Power Analysis* (SPA) y *Differential Power Analysis* (DPA) [6]. Las tarjetas inteligentes usan en los procesos criptográficos los algoritmos de encriptación simétricos como el *Advanced Encryption Standard* (AES) [19] y el *Data Encryption Standard* (DES) [21], los cuales son vulnerables frente a estos tipos de ataque.

En el presente capítulo se presenta el concepto de tarjeta inteligente. Luego, se menciona el funcionamiento del algoritmo DES. Posteriormente, se muestran los principales tipos de ataques que este tipo de tarjeta sufre. Finalmente, se presentan soluciones para disminuir la eficiencia de estos ataques.

1.2 TARJETAS INTELIGENTES

Se denomina tarjeta inteligente a cualquier tarjeta que tenga incorporada en su estructura un circuito integrado. Las tarjetas inteligentes presentan la misma apariencia física de una tarjeta de crédito o de una tarjeta SIM o GSM, pero internamente presentan las siguientes estructuras [1]:

- CPU: en la mayoría de modelos suele ser de 8 bits.
- Memoria ROM: esta tiene una capacidad de 12 a 30 KB en donde se aloja el sistema operativo de la tarjeta y el algoritmo de seguridad.
- Memoria EEPROM: memoria de almacenamiento en donde se ubican los ficheros y contraseñas de seguridad.
- Memoria RAM: memoria volátil asignada al procesador.

Según el estándar ISO/IEC 7816-3 [20], las tarjetas inteligentes se pueden clasificar según su rango de voltaje de alimentación. En la Tabla 1.1 se muestra las tres clases de tarjetas con su respectiva frecuencia de trabajo.

Tabla 1.1: Clasificación de las tarjetas inteligentes [20].

Clasificación de Tarjetas Inteligentes	Rango de voltaje de alimentación	Rango de frecuencia de trabajo del microprocesador
Clase A	5V +/-10%	1-5MHz
Clase B	3V +/-10%	1-5MHz
Clase C	1.8V +/- 10%	1-5MHz

1.3 DATA ENCRYPTION STANDARD (DES)

El DES es el algoritmo de encriptación más usado en tarjetas inteligentes. Desde hace tres décadas, este estándar ha tenido un papel importante en aplicaciones de seguridad de información, especialmente luego de ser aceptado por la *Federal Information Processing Standard* (FIPS) en noviembre de 1997. La Figura 1.1 muestra el esquema general de este algoritmo.

El DES usa numerosas secuencias de operaciones y permutaciones aplicadas a bloques de información. Este algoritmo opera con 16 *keys* (llaves) de 56 bits y divide la información original (*plaintext*) en bloques de 64 bits. Luego, estos bloques son divididos en dos sub-

bloques, inicialmente denominados L_0 y R_0. Se procede a ejecutar una función lógica, que tiene como parámetros la llave K_1 y el sub-bloque R_0. A continuación, se realiza una operación *xor* entre L_0 y el resultado de la función lógica f, y se genera el sub-bloque R_1. Este procedimiento se repite 16 veces, como se muestra en la Figura 1.1. Finalmente, se obtiene la información encriptada (*ciphertext*).

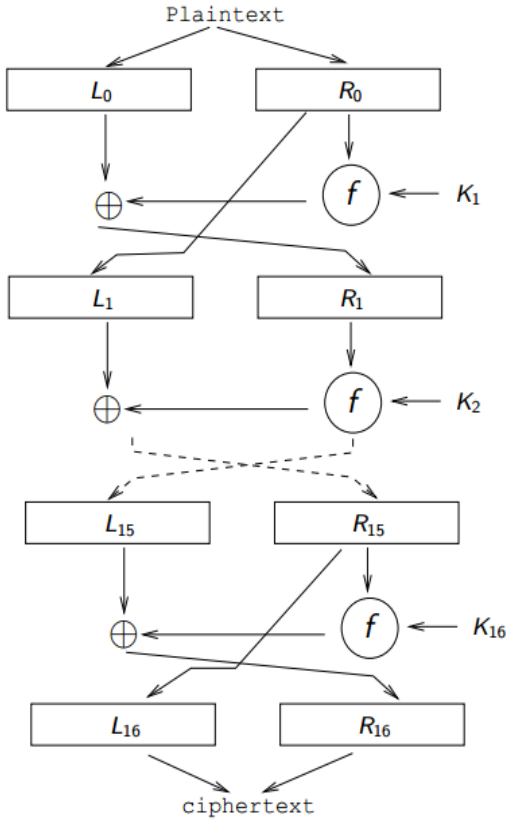

Figura 1.1: Esquema general del algoritmo DES [12].

1.4 TIPOS DE ATAQUES A TARJETAS INTELIGENTES

1.4.1 Simple Power Analysis (SPA)

Esta técnica toma como base de funcionamiento la medición e interpretación directa de la potencia consumida por algún procesador criptográfico. Los dispositivos vulnerables ante este tipo de ataque son aquellos que presentan un gran consumo de potencia [6].

Por ejemplo, en la Figura 1.2 se muestra la señal de corriente consumida por el procesador criptográfico de una tarjeta inteligente durante ciclos de reloj distintos. Las diferencias que presentan ambas muestras son debidas a las variaciones en las instrucciones realizadas por

el microprocesador. Estas solo difieren en el sexto ciclo de reloj. Esta diferencia se traduce en la variación de consumo de potencia del microprocesador.

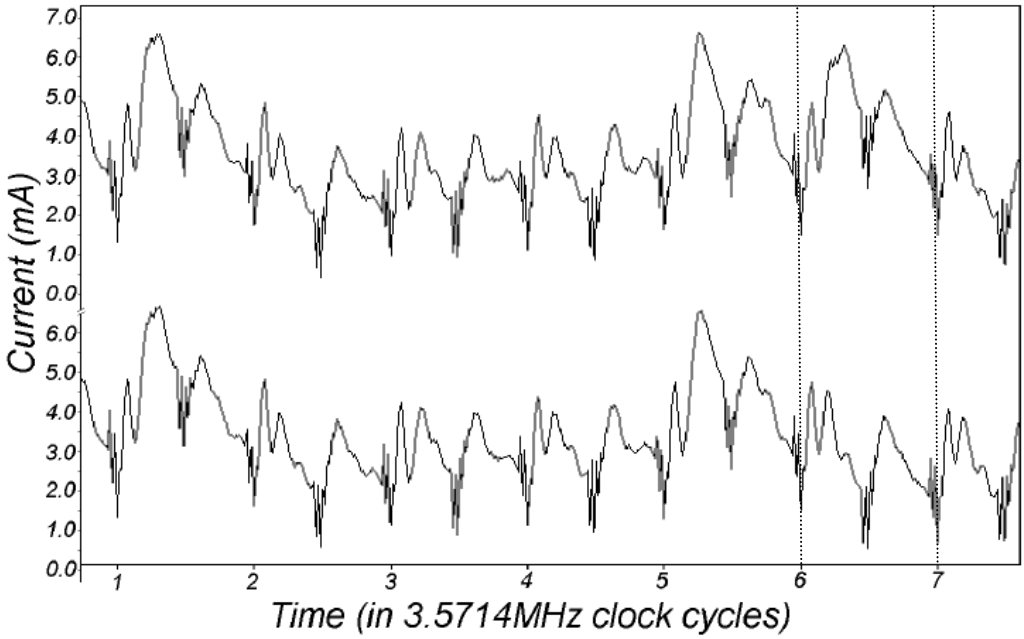

Figura 1.2: Variaciones de consumo de corriente de una tarjeta inteligente [6].

Para medir la potencia consumida se puede conectar una resistencia entre la fuente de alimentación y el terminal de alimentación de la tarjeta. De esta manera, se mide la caída de potencial en la resistencia con la ayuda de equipos con gran valor de muestreo (mayor a $1GHz$) [6]. La corriente consumida por la tarjeta se calcula por medio de la ley de Ohm.

1.4.2 Differential Power Analysis (DPA)

Este tipo de ataques es el más difundido y basa su funcionamiento en el análisis estadístico de la señal de consumo de potencia. El objetivo de este ataque es identificar todas las llaves (K_n) utilizadas durante una operación DES por medio de una función de selección [6].

En la parte superior de la Figura 1.3 se muestra una señal de corriente obtenida durante una operación DES (similar al ataque SPA), mientras que las demás son señales diferenciales obtenidas en base a una función de selección [6]. En base a la señal de referencia, se realizaron tres intentos para diferentes valores de K_n. El primer intento se realizó con un valor correcto de K_n. Se pueden apreciar picos de corriente en la muestra diferencial. Para los demás casos, el valor de K_n es incorrecto. Se puede distinguir que la señal diferencial

está en el orden de los microamperios y que el ruido es considerable frente a los picos mostrados.

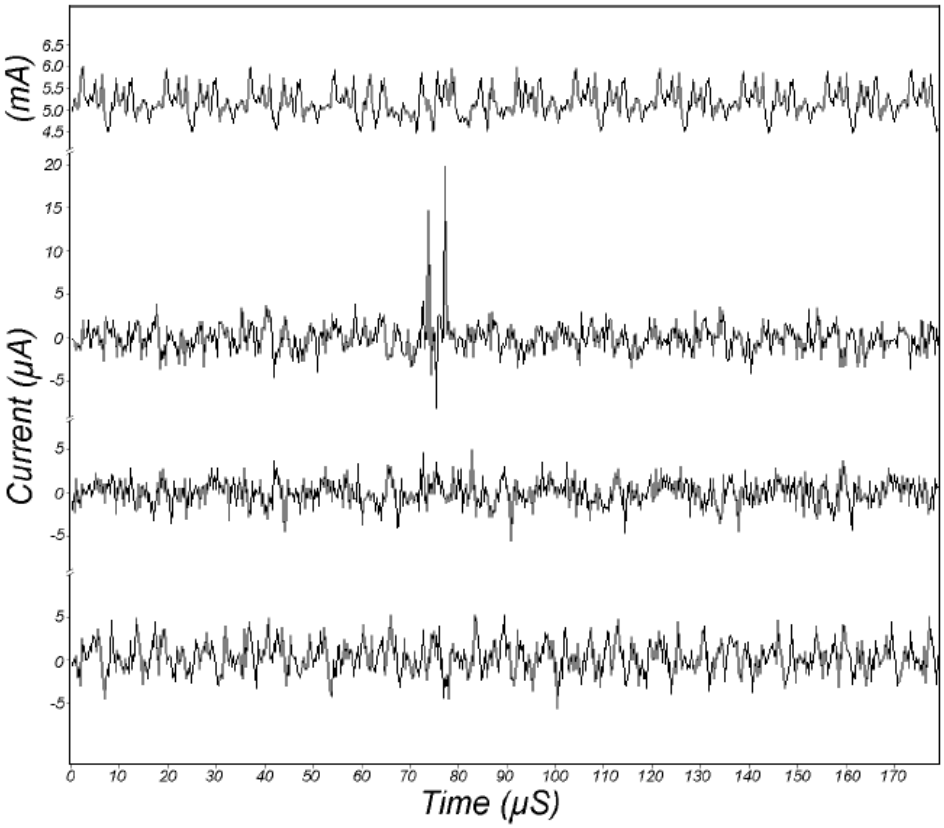

Figura 1.3: Muestras diferenciales de un ataque DPA [6].

1.5 MÉTODOS DE PROTECCIÓN ANTE ATAQUES DPA

1.5.1 Inserción de ruido

Implica insertar ruido en las muestras de corriente obtenidas. Generalmente, el ruido añadido es del tipo Blanco para que la correlación con la señal medida sea casi nula. Esta medida de seguridad fuerza al atacante a obtener una mayor cantidad de muestras. Sin embargo, esta solución es deficiente si se incrementa la relación señal a ruido de las muestras obtenidas [6].

1.5.2 Desincronización temporal

Esta medida de seguridad basa su funcionamiento en la variación aleatoria de la frecuencia de trabajo del dispositivo. En un ataque DPA, el pico respectivo a una comparación exitosa en la curva diferencial se verá ensanchado gracias a la desincronización realizada. Esto

deteriorará la relación señal a ruido de las muestras. Como contramedida, se plantea que para poder realizar un ataque DPA, una vez que los ciclos de cada muestra sean reconocidos, estos pueden ser ensanchados o comprimidos para normalizar todas las muestras [14].

1.5.3 Enmascaramiento algorítmico

Esta técnica sugiere enmascarar todos los resultados obtenidos luego del proceso de encriptación con la división de estos en k particiones. Esto logrará que la dificultad de obtener un ataque DPA exitoso se eleve exponencialmente k veces. Sin embargo, exige que el algoritmo de seguridad sea modificado. Este método es efectivo frente a ataques DPA de orden mínimo, pero vulnerable frente a ataques DPA más exhaustivos [14].

1.5.4 Atenuación de corriente

Esta técnica es la más difundida en la actualidad. En [7], [8], [9] y [11] se mencionan diversas formas de implementar esta técnica. El principal objetivo de esta es la reducción del nivel RMS de la corriente consumida por el microprocesador. De esta manera, la cantidad de muestras necesarias para atacar una tarjeta inteligente se eleva considerablemente, tal como se muestra en [17]. Su disposición en la tarjeta inteligente se muestra en la Figura 1.4.

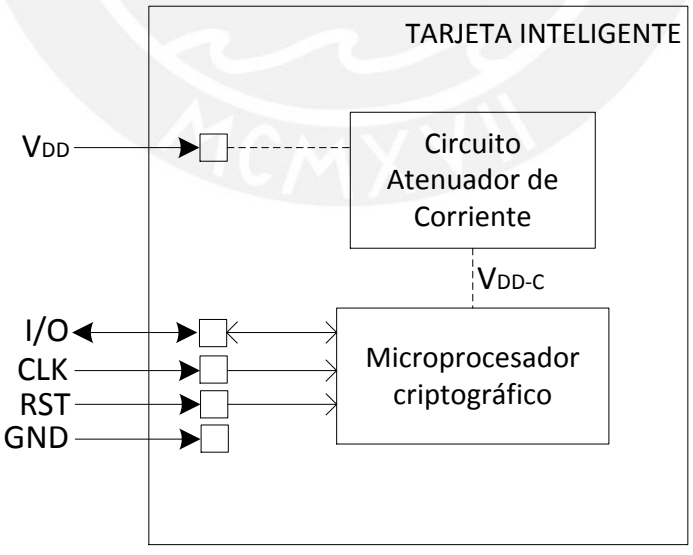

Figura 1.4: Ubicación del circuito de protección [9].

CAPÍTULO 2

TECNOLOGÍA CMOS Y ARQUITECTURA DE BLOQUES ANALÓGICOS INVOLUCRADOS EN LA TOPOLOGÍA PROPUESTA

2.1 INTRODUCCIÓN

En el presente capítulo se presentan los fundamentos teóricos sobre los cuales se desarrolla la presente tesis. Se muestra la teoría básica detrás del funcionamiento del transistor MOSFET y los fenómenos que ocurren dentro de su estructura bajo la presencia de voltajes en los terminales del mismo. Luego, se presenta la topología a usar y se establecen los requerimientos necesarios para inhabilitar ataques DPA sobre tarjetas inteligentes. Finalmente, se define la arquitectura del circuito a diseñar.

2.2 TECNOLOGÍA CMOS

Su invención se remonta alrededor del año 1930, cuando la idea de lo que sería posteriormente llamado transistor MOS, fue desarrollada por J. E. Lilienfeld. Sin embargo, su demostración funcional fue realizada en los años 60's por Kahng y Atalla [3].

La tecnología CMOS (*Complementary Metal-Oxide Semiconductor*) basa su funcionamiento en la propiedad complementaria que exhiben los transistores pMOS y nMOS. El uso

conjunto de ambos tipos de transistores MOS ofrece muchas ventajas con respecto a la tecnología TTL, tales como alta densidad de integración, escalamiento dimensional, bajo consumo de potencia estática, robustez frente a ruido, etc. Es por ello que, a partir de la década de los 80's, la tecnología CMOS superó a la tecnología TTL, especialmente en la implementación de circuitos integrados [3].

2.3 TRANSISTOR MOSFET

2.3.1 Estructura y funcionamiento

El transistor MOSFET (*Metal Oxide Semiconductor Field Effect Transistor*) es la unidad sobre la cual se basa la tecnología CMOS. Este dispositivo semiconductor basa su funcionamiento en el efecto de campo eléctrico, que afecta a los portadores de carga presentes en su estructura, al aplicarle tensiones a sus terminales. Existen dos tipos de transistores MOS: nMOS y pMOS. La diferencia entre ellos es el tipo de portadores mayoritarios que transportan por el canal.

Su estructura está conformada por cuatro terminales, los cuales son: Compuerta o *Gate* (G), Drenador o *Drain* (D), Surtidor o *Source* (S) y Substrato o *Bulk* (B). La Figura 2.1 muestra la estructura básica de un transistor nMOS y la simbología de este dispositivo semiconductor.

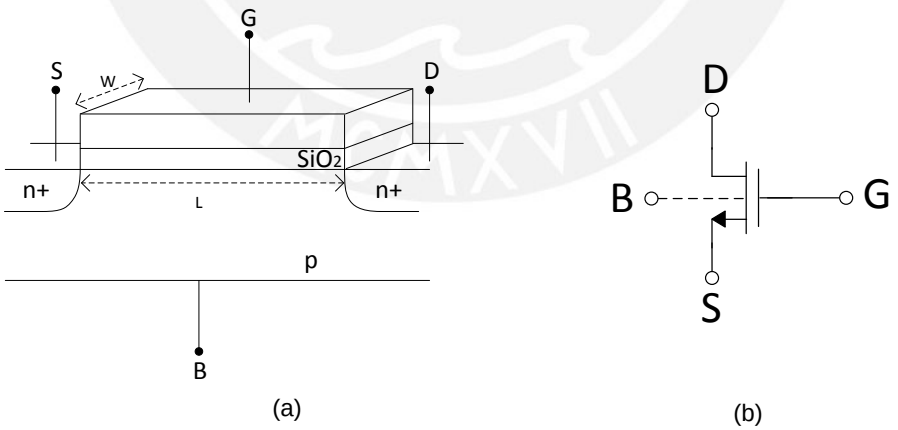

Figura 2.1: (a) Estructura del transistor nMOS. (b) Representación simbólica del transistor nMOS [3].

En el caso del transistor nMOS, el sustrato de material tipo-p sirve como superficie para la difusión de pozos de material tipo-n^+. Entre dichos pozos se crea una capa de óxido de Silicio. Finalmente, sobre esta última se deposita una capa de polisilicio (SiO_2).

Siguiendo con el caso del transistor nMOS, al aplicar una tensión positiva entre la compuerta y el substrato, se induce una carga negativa electrostática en la interfaz óxido-semiconductor. Este fenómeno repele a los huecos presentes en el substrato, creando una zona de agotamiento. Si el potencial en la compuerta aumenta, se puede lograr que la densidad de electrones que se encuentran en la superficie del substrato (zona de inversión) supere a la densidad de huecos del mismo. A la tensión de compuerta con la cual se logra alcanzar esta condición se le denomina Voltaje Umbral, V_{TH} . De esta forma, se formará una capa de portadores entre el drenador y el surtidor, denominada canal. Finalmente, el flujo de estos portadores dependerá de la tensión entre drenador y surtidor ,V_{DS} .

Por otro lado, el comportamiento del transistor MOSFET puede ser modelado matemáticamente. Uno de estos modelos es el denominado Modelo cuadrático o *Level 1* [2]. A continuación, se presentan las ecuaciones pertenecientes a dicho modelo:

Corte:

$$I_D = 0\,, \qquad V_{GS} \le V_{TH} \tag{2.1}$$

Región Lineal:

$$I_D = \mu_n C_{ox} \frac{W}{L}\left[(V_{GS} - V_{TH})V_{DS} - \frac{V_{DS}^2}{2}\right], \qquad V_{GS} > V_{TH} \text{ y } V_{DS} < V_{GS} - V_{TH} \tag{2.2}$$

Saturación:

$$I_D = \frac{1}{2}\mu_n C_{ox} \frac{W}{L}(V_{GS} - V_{TH})^2\,, \qquad V_{GS} > V_{TH} \text{ y } V_{DS} > V_{GS} - V_{TH} \tag{2.3}$$

Donde

I_D : Corriente de drenador

V_{TH} : Voltaje umbral

V_{GS} : Voltaje compuerta-surtidor

V_{DS} : Voltaje drenador-surtidor

μ_n : Movilidad de los electrones

C_{ox} : Capacitancia del óxido de compuerta

W : Ancho del canal del transistor

L : Largo del canal del transistor

Como se puede apreciar, el funcionamiento del transistor nMOS muestra una fuerte dependencia con respecto a las dimensiones del canal. A la relación (W/L) se le denomina el factor de forma.

Para el caso de los transistores pMOS, las ecuaciones (2.2) y (2.3) deberán ser modificadas teniendo en cuenta que, por convención, se asume que la corriente I_D fluye desde el drenador hacia el surtidor, mientras que los huecos fluyen en la dirección contraria.

Por otro lado, una de las propiedades más importantes de los transistores MOSFET es la transconductancia g_m. Esta nos brinda información acerca de la sensibilidad que presenta el dispositivo ante variaciones en su voltaje de compuerta, cuyo efecto se ve reflejado en la corriente de drenador. En [2] se define como:

$$g_m = \left.\frac{\delta I_D}{\delta V_{GS}}\right|_{VDS,const} \tag{2.4}$$

De (2.3):

$$g_m = \mu_n C_{ox} \frac{W}{L}\left(V_{GS} - V_{TH}\right) \tag{2.5}$$

También se cumple que:

$$g_m = \sqrt{2\mu_n C_{ox} \frac{W}{L} I_D} \tag{2.6}$$

$$= \frac{2I_D}{V_{GS} - V_{TH}} \tag{2.7}$$

2.3.2 Efectos de segundo orden

Efecto de cuerpo

Este fenómeno ocurre cuando la tensión V_{SB} es diferente de cero. Para el caso de un transistor nMOS, si tenemos $V_G < V_{TH}$ y $V_D = V_S = 0$, entonces en el substrato no existirá una capa de inversión. Si $V_B < 0$, entonces una mayor cantidad de huecos serán atraídos a la conexión del substrato y el ancho de la zona de agotamiento se incrementará. Esto

causará que el voltaje umbral se incremente. A este fenómeno se le llama efecto de cuerpo. En [3] se muestra que:

$$V_{TH} = V_{TO} + \gamma(\sqrt{|2\phi_F + V_{SB}|} - \sqrt{|2\phi_F|}) \quad (2.8)$$

Donde

V_{TO} : Voltaje umbral cuando V_{SB} es cero

γ : Coeficiente del efecto de cuerpo

ϕ_F : Voltaje de Fermi

V_{SB} : Voltaje surtidor-substrato

Generalmente, este efecto es indeseable ya que complica el diseño de circuitos analógicos y digitales [2].

Modulación de longitud de canal

En la región de saturación, la longitud de canal decrece conforme aumenta el voltaje V_{DS} . A este fenómeno se le denomina modulación de longitud de canal. Se tiene en saturación [3]:

$$I_D \approx \frac{1}{2}\mu_n C_{ox}\frac{W}{L}(V_{GS} - V_{TH})^2(1 + \lambda V_{DS}) \quad (2.9)$$

Donde

λ : Coeficiente de modulación de longitud de canal

Este fenómeno genera que, en saturación, el transistor no se comporte como una fuente de corriente ideal ya que λ inserta una pendiente en la curva característica I_D / V_{DS} .

2.4 TOPOLOGÍA UTILIZADA EN NUESTRO ESTUDIO

De acuerdo con el estado del arte, actualmente existen soluciones a nivel hardware y software. Para el presente trabajo se tomó en cuenta aquellas soluciones que impliquen el diseño analógico de circuitos integrados. De este grupo de soluciones, la más difundida y usada para inhabilitar ataques DPA es la técnica llamada Atenuación de Corriente. Esto se debe a las siguientes razones:

- La implementación de esta técnica puede lograrse sin modificar la estructura del procesador criptográfico ni la lógica programada del mismo.
- El incremento del número de muestras necesarias para un ataque DPA efectivo está relacionado directamente al porcentaje de atenuación logrado [17].
- Consumo mínimo de recursos, tales como potencia y área ocupada.

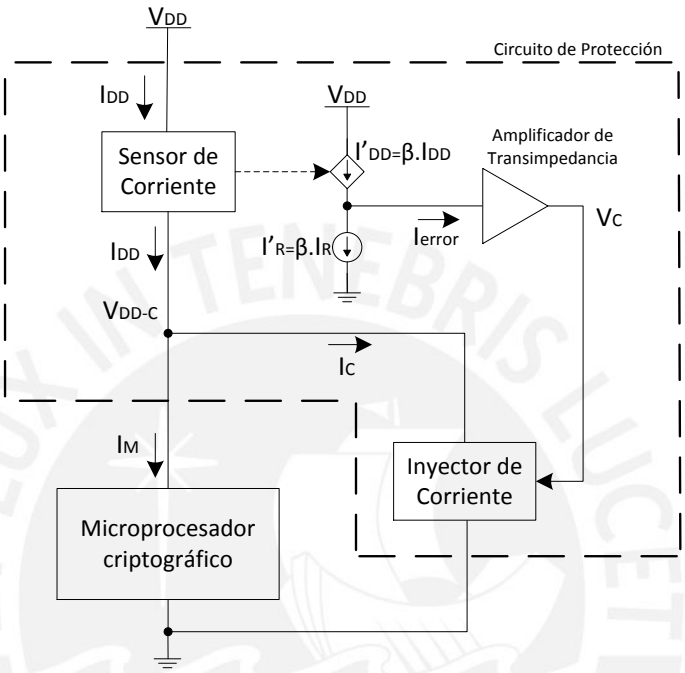

Figura 2.2: Diagrama de bloques de la técnica Atenuación de Corriente [7]

La Figura 2.2 presenta el diagrama de bloques básico de la técnica Atenuación de Corriente. El sensor de corriente mide la corriente I_{DD} que pasa por el terminal V_{DD} de la tarjeta inteligente. Este sensor brinda una versión atenuada de esta corriente, denominada I'_{DD}, la cual es comparada con una versión atenuada de la corriente de referencia I'_R. El resultado es inyectado al amplificador de transimpedancia. Este proporcionará a su salida la señal de voltaje V_C, la cual controlará al inyector de corriente. Cuando $I_{DD} < I_R$, el inyector de corriente incrementará I_C y permitirá que I_{DD} se mantenga cercano a I_R.

Como se puede observar, la topología utilizada en el presente trabajo puede ser segmentada en tres bloques principales: Sensor de corriente, Amplificador de Transimpedancia y el Inyector de corriente. A continuación, se presentan los requerimientos para que esta técnica sea efectiva y se define la estructura de cada uno de los bloques mencionados.

2.4.1 Requerimientos

En el presente trabajo, se utilizará la tecnología AMS 0.35 μm, la cual emplea un voltaje de alimentación típico de $3.3V$ [23]. Es por ello que, en base a la clasificación expuesta en el Capítulo 1, se decidió diseñar el circuito de protección aplicado a tarjetas inteligentes de Clase B.

El número de muestras que se requiere para poder efectuar un ataque DPA efectivo (más conocido como NCT-DPA) es utilizado para medir la robustez de un sistema ante este tipo de ataques. En [17] se propone una fórmula que relaciona los niveles RMS de la señal de corriente consumida por un microsistema durante la ejecución de un algoritmo criptográfico y el valor NCT-DPA. Asimismo, esta fórmula puede ser relacionada con el porcentaje de atenuación logrado por el circuito a diseñar. A continuación se presenta la ecuación mencionada.

$$N = \left(4 \frac{\sqrt{\frac{5}{6} \cdot (i_{dd})^2 + (i_{ext})^2} + i_{ext}}{0.23 \cdot i_{dd}} \right)^2 \tag{2.10}$$

Donde:

N : Número de muestras que se requiere para poder efectuar un ataque DPA efectivo

i_{dd} : Valor RMS de la señal atenuada de corriente

i_{ext} : Valor RMS del ruido externo

Por otro lado, el porcentaje de atenuación de corriente se puede expresar de la siguiente manera:

$$A = \left(\frac{i_c - i_{dd}}{i_c} \right) \cdot 100 \tag{2.11}$$

Donde:

A : Porcentaje de atenuación logrado con el circuito de protección

i_c : Nivel RMS de la señal original de corriente

i_{dd} : Valor RMS de la señal atenuada de corriente

En [17] se muestra que el NTC-DPA para un sistema sin protección equivale a 400 muestras. Por lo tanto, para que el circuito de protección sea efectivo se debe lograr que el NTC-DPA sea mayor a 400 muestras.

Debemos de tener en cuenta las características de la señal de corriente consumida por el procesador criptográfico. En el presente trabajo asumiremos que esta señal varía entre $2mA$ y $8mA$ (tomando en cuenta lo propuesto en [7], [8], [9], [11] y [14]) con una frecuencia máxima de $5MHz$ (frecuencia máxima de trabajo del procesador). Por lo tanto, el nivel RMS de la señal original de corriente será $i_{dd} = 2.12 \times 10^{-3} A$. A partir de [17], podemos asumir que $i_{ext} = 2 \times 10^{-4} A$.

En base al análisis desarrollado, se concluye que el nivel de atenuación debe ser mayor a 81% para obtener un valor de NTC-DPA mayor a 400 muestras.

Por otro lado, comparando los resultados obtenidos en [7], [8] y [9], se decide que el circuito a diseñar debe presentar un consumo de potencia menor a $40mW$.

Finalmente, se define que el ancho de banda sea mayor a $5MHz$ para poder asegurar la atenuación de corriente en todo el espectro de frecuencias posibles de la señal de corriente consumida por el microprocesador criptográfico.

2.4.2 Bloques Analógicos involucrados

Sensor de corriente

Este bloque debe fijar el voltaje de alimentación requerido por el microprocesador. Por lo tanto, dicho voltaje debe ser medido y comparado con un voltaje de referencia. A partir de la diferencia entre ambas señales, ese bloque deberá aumentar o disminuir el voltaje de alimentación del procesador. Por otro lado, este sensor debe otorgar una versión atenuada de la corriente que consume el microprocesador. Esto se puede lograr por medio de un espejo de corriente.

Se utiliza un amplificador diferencial con carga activa, ya que la salida de este sensor debe ser de un solo terminal. Asimismo, en [2] se recomienda usar este tipo de amplificador conjuntamente con un lazo de retroalimentación. Esto se logra por medio de un transistor pMOS, cuya compuerta será controlado por la salida de este bloque.

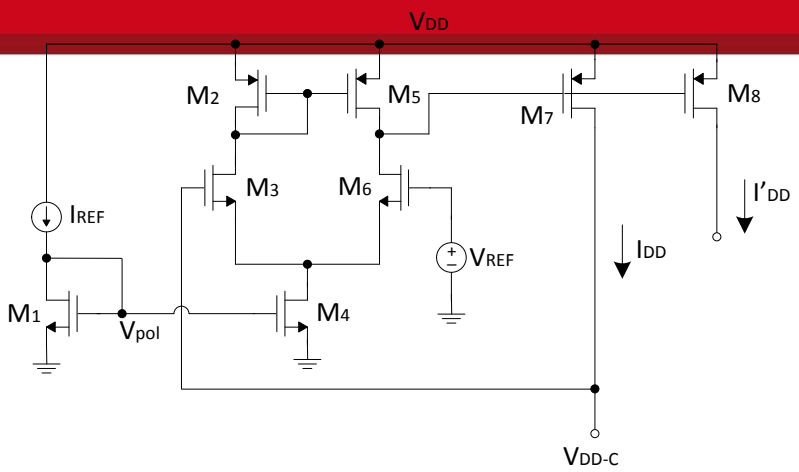

Figura 2.3: Esquemático del sensor de corriente [7].

A partir de la Figura 2.3, los transistores $M2$, $M3$, $M4$, $M5$ y $M6$ constituyen el amplificador diferencial con carga activa. La señal V_{DD-C} es comparada con el voltaje de referencia V_{REF}. El objetivo es lograr una caída de voltaje constante entre el drenador y surtidor de $M7$ y asegurar el correcto funcionamiento del microprocesador.

Amplificador de transimpedancia

Este bloque permite la conversión de la señal de error I_{error} en la señal de voltaje V_C. En la Figura 2.4 se muestra el circuito esquemático de este bloque. Este define la respuesta en frecuencia del circuito de protección. Debido a su estructura se reconocen dos nodos importantes, los cuales están asociados con el polo dominante y no dominante del circuito. En el siguiente capítulo se muestran las ecuaciones que gobiernan el comportamiento en frecuencia de este bloque.

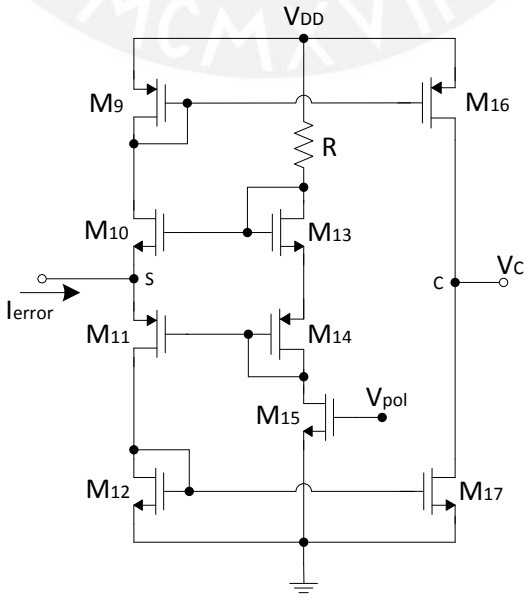

Figura 2.4: Esquemático del amplificador de transimpedancia [7].

Inyector de corriente

Consta de un solo transistor y es controlado por el voltaje de salida del amplificador de transimpedancia. Cuando el microprocesador de la tarjeta inteligente incremente su consumo de corriente, la señal de error aumenta, logrando que la señal V_C disminuya. Por lo tanto, el inyector de corriente disminuye su capacidad de corriente; es decir, I_C disminuirá. De esta manera, se logra que la señal de corriente vista desde la fuente de alimentación se mantenga cercana a la corriente de referencia.

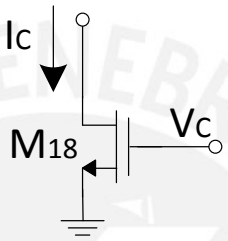

Figura 2.5: Esquemático del inyector de corriente [7].

CAPÍTULO 3

DISEÑO DEL CIRCUITO DE PROTECCIÓN

3.1 INTRODUCCIÓN

En el presente capítulo se muestra el diseño del circuito de protección. Se busca encontrar los valores de polarización y las dimensiones de los transistores que conforman el circuito. Luego de definir estos parámetros, se procede a realizar las simulaciones pertinentes con ayuda del software Cadence y se verifica si se obtienen los resultados esperados. Posteriormente, se elabora el *layout* físico del mencionado circuito con tecnología AMS 0.35 μm. Por lo tanto, se mencionan las principales reglas para la elaboración del *layout*. Se debe tener en cuenta que el análisis del circuito de protección se basa en los criterios mencionados en el Capítulo 2.

3.2 OBJETIVOS

3.2.1 Objetivo general

Diseñar un circuito capaz de incrementar la seguridad frente ataques del tipo DPA sobre tarjetas inteligentes de Clase B mediante la atenuación de variaciones de consumo de corriente.

3.2.2 Objetivos específicos

- Asegurar que el voltaje de alimentación del microprocesador criptográfico sea igual a $3V$ pese a las variaciones de consumo.
- Lograr una atenuación de variaciones de consumo de corriente mayor a 81%.
- Obtener un ancho de banda mayor a $5MHz$.
- Lograr un consumo de potencia menor a $40mW$.
- Elaborar el layout del circuito diseñado.

3.3 ESQUEMA GENERAL DE DISEÑO

En la Figura 3.1 se presenta el diagrama esquemático del circuito a diseñar. Uno de los objetivos es mantener el voltaje V_{DD-C} en $3V$. Este valor de voltaje es esencial para todo el circuito. Por este motivo, el primer bloque diseñado es el sensor de corriente. Luego, se procede a diseñar el amplificador de transimpedancia y el inyector de corriente. Por medio del análisis en frecuencia y el porcentaje de atenuación de las variaciones de consumo de corriente del microprocesador criptográfico se determinará la eficiencia del circuito diseñado.

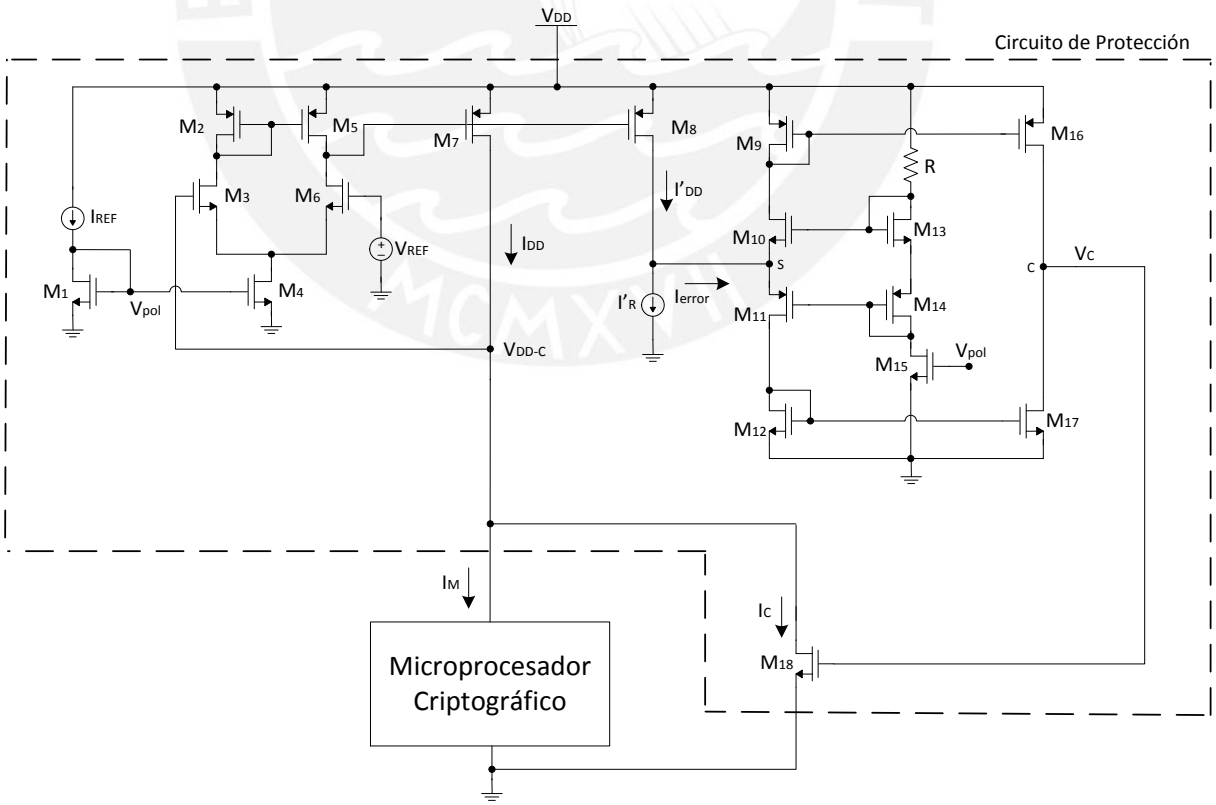

Figura 3.1: Esquemático del circuito de protección [7].

3.3.1 Modelos del transistor MOS para el diseño analógico

Actualmente, existen modelos matemáticos tales como el BSIM, EKV, PSP o el ACM [3] que describen el comportamiento de los transistores MOSFET. Para el circuito a diseñar se requiere de un modelo que presente las siguientes características:

- Proveer expresiones matemáticas sencillas para facilitar el diseño de circuitos analógicos.
- Modelar las cargas capacitivas propias de la estructura de los transistores MOS.
- Presentar simetría geométrica entre los terminales drenador y surtidor.

El modelo cuadrático cumple con estos requisitos y brinda ecuaciones sencillas de manejar. Por otro lado, los fabricantes de circuitos integrados utilizan el modelo BSIM. Este modelo logra controlar con mayor eficiencia los diferentes fenómenos que ocurren dentro de la estructura del transistor MOS, pero a costa de una mayor cantidad de variables y ecuaciones con un gran nivel de complejidad.

Por esta razón, en la primera parte del diseño se utilizará el modelo cuadrático. Esto facilita los cálculos manuales que serán necesarios para hallar los factores de forma de los transistores. Posteriormente, con la ayuda del software Cadence podremos obtener los factores de forma con mayor precisión de cálculo basándonos en simulaciones. Esto se debe a que este software utiliza el modelo BSIM3v3.

3.3.2 Flujo de diseño de circuitos integrados analógicos

En los últimos años, el diseño de circuitos integrados se ha visto altamente afectado por el escalamiento que presentan las dimensiones de los transistores. Es por ello que el diseño de circuitos integrados radica principalmente en la obtención de los factores de forma de los transistores que participan en un circuito determinado.

La Figura 3.2 muestra el diagrama de flujo básico que se seguirá para el diseño del circuito de protección. En primer lugar, se selecciona el modelo de transistor. Luego, en base a los requerimientos del circuito se seleccionan los factores de forma de los transistores. A continuación, se procede a realizar las simulaciones y se verifica el cumplimiento de los objetivos. Seguidamente, se procede al desarrollo del *layout* físico. Finalmente, se realizan las pruebas *post-layout* y se verifica el funcionamiento del circuito tomando en cuenta características parásitas propias de la estructura de los transistores MOS.

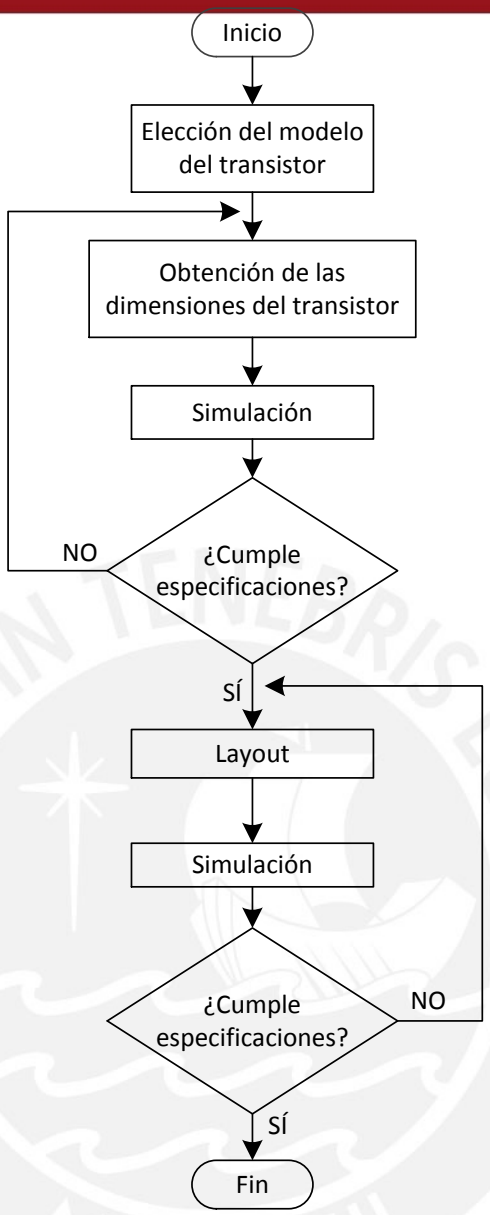

Figura 3.2: Diagrama de flujo del diseño del circuito de protección.

3.4 LAZO DE CONTROL DE ATENUACIÓN

El objetivo del lazo de control es compensar las variaciones de la señal de corriente I_{DD} y lograr que sea similar a la corriente de referencia I_R. Para ello, se utilizó el lazo de control que se muestra en la Figura 3.3. Se pueden apreciar los distintos bloques involucrados y la ganancia de cada uno de ellos. A partir del gráfico, se establece que:

$$I_{DD} = \frac{GR\beta}{1+GR\beta} I_R + \frac{1}{1+GR\beta} I_M \tag{3.1}$$

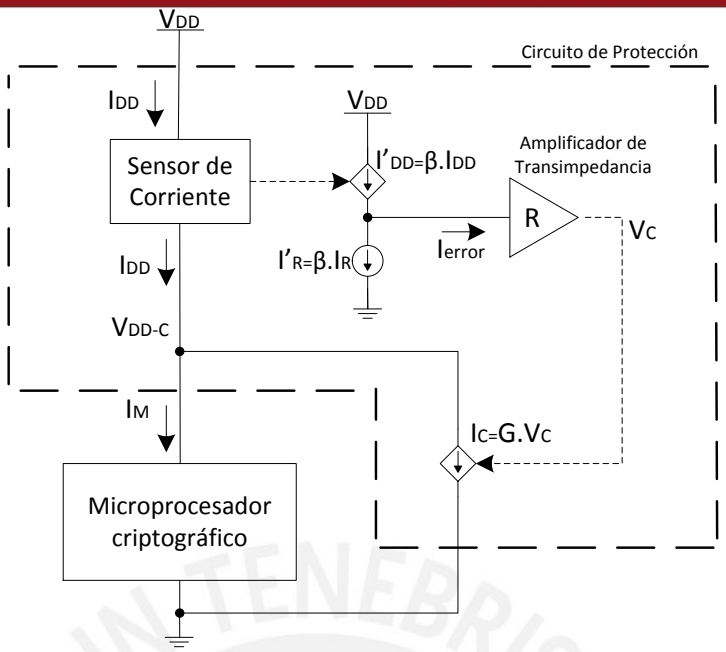

Figura 3.3: Lazo de control de atenuación de corriente [9].

A partir de la ecuación (3.1) se puede afirmar que con una alta ganancia de lazo , es decir $GR\beta >> 1$, podremos asegurar que I_{DD} seguirá a I_R.

A continuación, se exponen las ecuaciones que definen el funcionamiento de cada bloque del circuito de protección y se definen los factores de forma de los transistores que lo conforman.

3.4.1 Sensor de corriente

En el capítulo anterior, se discutió acerca de las funciones de este bloque. Estas son:

- Mantener el voltaje de alimentación V_{DD-C} del microprocesador a $3V$.
- Copiar la corriente de consumo I_{DD}.

A continuación se exponen los análisis necesarios para el diseño de este bloque.

Análisis en gran señal

Los transistores que conforman el sensor de corriente deben trabajar en la región de saturación si deseamos obtener una ganancia de voltaje diferencial. Asimismo, el transistor

$M7$ (Figura 3.1) deberá lograr que el voltaje V_{DD-C} sea igual a $3V$. Para ello, fijaremos el voltaje V_{SD7} a $300mV$, teniendo en cuenta que $V_{DD} = 3.3V$.

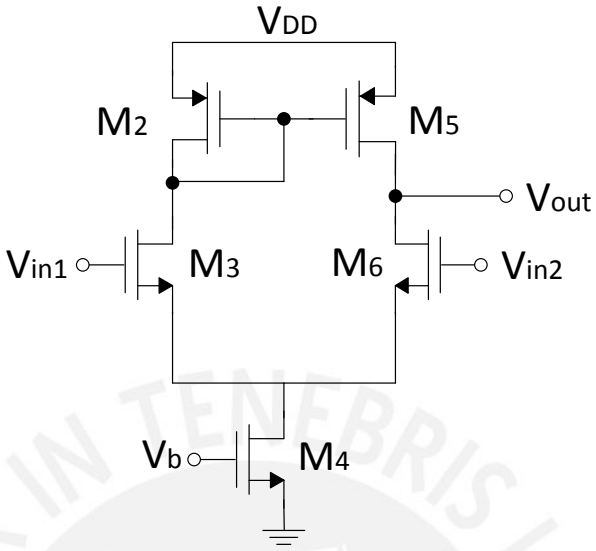

Figura 3.4: Esquemático del amplificador diferencial con carga activa [2].

En base a la Figura 3.4, conforme V_{in1} se aproxima a V_{in2}, $M3$ se enciende y fluye corriente desde $M2$ hasta $M4$. Este último transistor copia esa corriente a $M5$ y lo enciende. Entonces, el voltaje de salida dependerá del cambio del potencial V_{DS6} que se genera a partir de la modulación de la longitud del canal de $M6$. Para una pequeña diferencia entre V_{in1} y V_{in2}, los transistores $M5$ y $M6$ estarán saturados y proveerán una gran ganancia [2].

El voltaje en modo común deberá permitir que $M6$ esté en saturación. Por ello:

$$V_{OUT} > V_{in.CM} - V_{TH} \tag{3.2}$$

Asimismo, cuando $V_{in1} = V_{in2}$:

$$V_{OUT} = V_{DD} - |V_{GS2}| \tag{3.3}$$

Para polarizar el amplificador diferencial hacemos uso del transistor $M4$. Este actúa como una fuente de corriente constante. Este a su vez, forma parte de un espejo de corriente, tal como se muestra en la Figura 3.5.

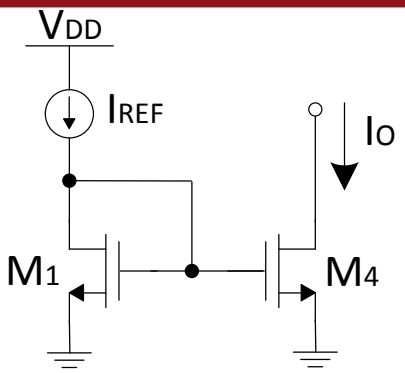

Figura 3.5: Esquemático del espejo de corriente [2].

A partir de la Figura 3.5 se obtiene:

$$I_O = \frac{(W/L)_4}{(W/L)_1} I_{REF} \tag{3.4}$$

La independencia sobre las variables de proceso es una ventaja que presentan los espejos de corriente. En la presente tesis se asume que la fuente de corriente es igual a $I_{REF} = 1\mu A$.

Por otro lado, debemos dimensionar los transistores $M7$ y $M8$ para que este bloque pueda copiar de manera eficiente la corriente I_{DD}. Para ello, se debe de tomar en cuenta que esta corriente fluctuará alrededor de la corriente de referencia I_R. Por lo tanto, el transistor $M7$ deberá ser capaz de manejar esta corriente manteniendo su voltaje V_{SD7} en $300mV$. Tenemos que:

$$I_{D7} = \mu_p C_{ox} \left(\frac{W}{L}\right)_7 \left[(V_{SG7} - |V_{TH}|) V_{SD7} - \frac{V_{SD7}^2}{2} \right] \tag{3.5}$$

$$\left(\frac{W}{L}\right)_7 = \frac{I_{D7}}{\mu_p C_{ox} \left[(V_{SG7} - |V_{TH}|) V_{SD7} - \frac{V_{SD7}^2}{2} \right]} \tag{3.6}$$

Como $M7$ y $M8$ conforman un espejo de corriente, ambos transistores definirán el factor β de la Figura 3.3. Este factor nos permitirá trabajar con corrientes en el orden de los μA. De esta forma, se logrará controlar el consumo de potencia del lazo de control.

Podemos asumir que:

$$\beta = \frac{1}{100} \tag{3.7}$$

Es decir:

$$\frac{(W/L)_8}{(W/L)_7} = \frac{1}{100} \tag{3.8}$$

Análisis en pequeña señal

El sensor de corriente está conformado por un amplificador diferencial con carga activa. De la Figura 3.4, $M2$ y $M5$ constituyen un espejo de corriente y al mismo tiempo, la carga del amplificador diferencial. El par diferencial está conformado por los transistores $M3$ y $M6$. El transistor $M4$ polariza el circuito ya que trabaja como una fuente de corriente.

En [2] se muestra que la ganancia en modo diferencial de este amplificador puede obtenerse a partir de la siguiente expresión:

$$A_{DM} = g_{m3.6}(r_{O3,6} \| r_{O2,5}) \tag{3.9}$$

En [2] y [3] se menciona que $M2$ y $M5$ deben ser idénticos. Asimismo, $M3$ y $M6$ también deben ser idénticos para copiar corriente de forma eficiente.

A partir de (2.6):

$$g_{m3,6} = \sqrt{2u_n C_{ox}\left(\frac{W}{L}\right)_{3,6} I_{D3,6}} \tag{3.10}$$

$$\left(\frac{W}{L}\right)_{3,6} = \frac{{g_{m3,6}}^2}{2u_n C_{ox} I_{D3,6}} \tag{3.11}$$

Análisis en frecuencia

Se pueden determinar dos caminos para las señales que interactúan dentro del amplificador, como se muestra en la Figura 3.6(a). El primero está definido por los transistores $M2$ y $M5$, los cuales estarán asociados con el nodo A, denominado el polo espejo. El segundo estará definido por los transistores $M3$ y $M6$, y es denominado el polo de salida, ubicado en el nodo B. En la Figura 3.6(b) se muestran las capacitancias asociadas a cada polo.

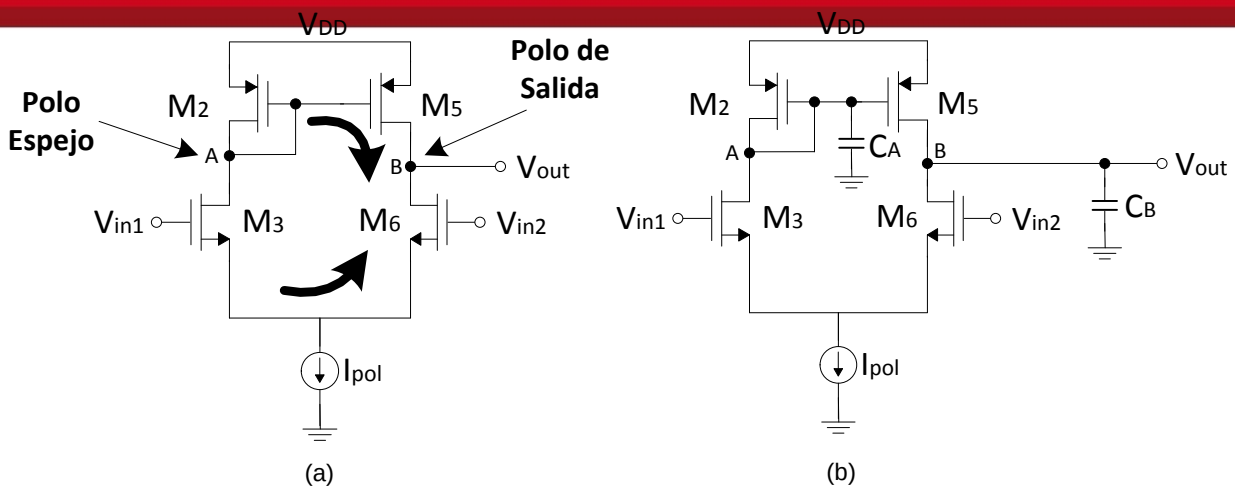

Figura 3.6: (a) Caminos de las corrientes [2]. (b) Capacitancias y nodos que definen los polos del amplificador diferencial con carga activa [2].

En [2] se determinan las siguientes expresiones para los polos mencionados:

Polo de salida: $$\omega_{p1} = \frac{1}{(r_{O5} \| r_{O6}) C_B} \tag{3.12}$$

Polo espejo: $$\omega_{p2} = \frac{g_{m2}}{C_A} \tag{3.13}$$

Donde C_A es la suma de las capacitancias C_{gs2}, C_{gs5}, C_{db2}, C_{db3} y el efecto Miller de C_{gd3} y C_{gd5}. La capacitancia C_B se genera debido a la carga definida por los transistores M_7 y M_8. Asumiendo que $1/(r_{O5} \| r_{O6}) << g_{m2}$, se determina que el polo de salida es menor que el polo espejo. Entonces, el polo de salida es el que definirá el ancho de banda. Como requerimiento del circuito de protección:

$$f_{p1} > 5MHz \tag{3.14}$$

$$\frac{1}{2\pi (r_{O5} \| r_{O6}) C_B} > 5MHz \tag{3.15}$$

Se puede definir como criterio de diseño que:

$$f_{p2} > 10 f_{p1} \tag{3.16}$$

$$g_{m2} > 10 \frac{C_A}{(r_{O5} \| r_{O6}) C_B} \tag{3.17}$$

3.4.2 Amplificador de transimpedancia

Se comienza por definir los puntos de operación de los transistores involucrados, luego se analizan las ecuaciones que gobiernan su ganancia, y finalmente determinamos su respuesta en frecuencia.

Análisis en gran señal

De la Figura 3.1, la rama de polarización de este bloque está constituida por los transistores $M13$, $M14$, $M15$ y $M1$, y la resistencia R. La corriente de polarización I_{REF} es copiada por medio del espejo de corriente formado por $M1$ y $M15$. Por lo tanto:

$$I_{D15} = \frac{(W/L)_{15}}{(W/L)_1} I_{REF} \tag{3.18}$$

Se cumple que:

$$I_{D13} = I_{D14} = I_{D15} = \frac{1}{2}\mu_n C_{ox}\left(\frac{W}{L}\right)_{13}(V_{GS13} - V_{TH})^2 \tag{3.19}$$

$$\left(\frac{W}{L}\right)_{13} = \frac{I_{D15}}{\frac{1}{2}\mu_n C_{ox}(V_{GS13} - V_{TH})^2} \tag{3.20}$$

$$\left(\frac{W}{L}\right)_{14} = \frac{I_{D15}}{\frac{1}{2}\mu_p C_{ox}(V_{SG14} - |V_{TH}|)^2} \tag{3.21}$$

Luego, por medio de $M13$ y $M14$ se brinda el voltaje de compuerta capaz de hacer trabajar en la región de saturación a la rama de entrada del amplificador. La resistencia presente en el circuito tiene como finalidad la calibración de voltaje y potencia de la rama de polarización.

Tenemos:

$$R = \frac{V_{DD} - V_{D13}}{I_{D15}} \tag{3.22}$$

Si se logra que $V_S = V_{S13} = V_{S14}$ entonces se cumple lo siguiente:

$$I_{D10} = \frac{(W/L)_{10}}{(W/L)_{13}} I_{D13} \tag{3.23}$$

$$I_{D11} = \frac{(W/L)_{11}}{(W/L)_{14}} I_{D14} \tag{3.24}$$

Tenemos que:

$$(W/L)_{10} = \frac{(W/L)_{13} I_{D10}}{I_{D13}} \tag{3.25}$$

$$(W/L)_{11} = \frac{(W/L)_{14} I_{D11}}{I_{D14}} \tag{3.26}$$

Los transistores $M9$ y $M16$ forman un espejo de corriente, por lo que se cumple:

$$I_{D16} = \frac{(W/L)_{16}}{(W/L)_{9}} I_{D9} \tag{3.27}$$

Para los transistores $M12$ y $M17$ se presentará la misma relación:

$$I_{D17} = \frac{(W/L)_{17}}{(W/L)_{12}} I_{D12} \tag{3.28}$$

Como $I_{D16} = I_{D17}$, tendremos que:

$$\frac{(W/L)_{16}}{(W/L)_{9}} I_{D9} = \frac{(W/L)_{17}}{(W/L)_{12}} I_{D12} \tag{3.29}$$

Análisis en pequeña señal

El análisis en pequeña señal del amplificador de transimpedancia se muestra en el Anexo 1. En base al procedimiento realizado en dicho anexo, tenemos que la ganancia R de este bloque es igual:

$$R = -\frac{(W/L)_{16}}{(W/L)_9} Z_{out} \tag{3.30}$$

Podemos ver que la proporción entre los factores de forma del espejo de corriente conformado por $M16$ y $M9$ influye de manera notoria en la ganancia del amplificador.

Asimismo, la impedancia de salida del mismo puede ser expresado como:

$$Z_{out} = r_{16} \,||\, r_{17} \tag{3.31}$$

Se debe de tomar en cuenta los criterios para la obtención de estas expresiones. En base a estos, debemos lograr que $g_{m10} >> g_{m11}$.

Análisis en frecuencia

En base a la estructura del amplificador se pueden diferenciar dos nodos importantes. Estos nodos están etiquetados como el nodo B y el nodo C, según la Figura A.1. La resistencia y la capacitancia asociadas a cada uno de estos nodos nos permitirán hallar la expresión de los polos que caracterizan la respuesta en frecuencia del amplificador. Obtenemos la siguiente función de transferencia:

$$\frac{v_{out}}{i_{error}} = -\frac{(W/L)_{16}(r_{16} \,||\, r_{17})}{(W/L)_9} \frac{1}{(1+(r_{16} \,||\, r_{17})C_C s)} \frac{1}{\left(1+\frac{C_B}{g_{m10}+g_{m11}} s\right)} \tag{3.32}$$

Se puede identificar la ganancia del amplificador a baja frecuencias, la cual es afectada por las capacitancias parásitas de los transistores conforme se eleva la frecuencia. Estas definen dos polos que están asociados a las siguientes frecuencias:

$$f_1 = \frac{1}{2\pi(r_{16} \,||\, r_{17})C_C} \tag{3.33}$$

$$f_2 = \frac{g_{m10}+g_{m11}}{2\pi C_B} \tag{3.34}$$

Donde f_1 es la frecuencia asociada al polo dominante, el cual se ubica en el nodo C.

La capacitancia C_C es igual a:

$$C_C = C_{gs18} + C_{gd18}A_{v18} + C_{gd16} + C_{gd17} \tag{3.35}$$

El polo ubicado en f_2 está asociado al nodo B. La capacitancia C_B es igual a:

$$C_B = C_{gs10} + C_{gs11} \tag{3.38}$$

3.4.3 Inyector de corriente

Este bloque está formado por el transistor $M18$. Este será controlado por el voltaje de salida V_c del amplificador de transimpedancia. Cuando esta señal aumente, entonces $M18$ absorberá una mayor cantidad de corriente. Esta corriente adicional logrará compensar las variaciones de consumo de corriente del microprocesador criptográfico. La relación entre la señal de control, V_c, y la corriente absorbida por $M18$, I_C, se define como la transconductancia de este transistor. Se puede expresar de la siguiente manera:

$$g_{m18} = \mu_n C_{ox}\left(\frac{W}{L}\right)_{18}(V_C - V_{TH}) \tag{3.39}$$

A partir de (3.39), se puede determinar que la señal de control es proporcional a las variaciones de corriente.

Para la elección del factor de forma de $M18$ se debe tomar en cuenta la ganancia del lazo cerrado, así como el ancho de banda del circuito de protección.

La ganancia de lazo se puede definir como el producto de la ganancia de los tres bloques en los cuales se dividió el circuito. A partir de (3.7), (3.30) y (3.39) obtenemos la siguiente expresión:

$$\frac{i_c}{i_{dd}} = \frac{i'_{dd}}{i_{dd}} \cdot \frac{v_c}{i'_{dd}} \cdot \frac{i_c}{v_c} \tag{3.40}$$

$$\frac{i_c}{i_{dd}} = \beta \cdot \frac{(W/L)_{16}}{(W/L)_9}(r_{16} \parallel r_{17}) \cdot g_{m18} \tag{3.41}$$

Por otro lado, la atenuación proporcionada por el circuito de protección puede ser expresada de la siguiente manera:

$$A = \left(\frac{i_c - i_{dd}}{i_c} \right) \cdot 100 \tag{3.42}$$

Donde

A: Porcentaje de atenuación logrado con el circuito de protección

i_c: Nivel RMS de la señal original de corriente

i_{dd}: Nivel RMS de la señal atenuada de corriente

Debemos expresar a la ecuación (3.42) en función de las dimensiones de los transistores que forman parte del circuito. Por lo tanto, de (3.41) tenemos:

$$A = \frac{i_c - i_c\left[\frac{(W/L)_9}{(W/L)_{16}(r_{16} \parallel r_{17}) g_{m18} \beta} \right]}{i_c} \cdot 100 \tag{3.43}$$

Asimismo, debemos recordar que uno de nuestros objetivos es lograr una atenuación de corriente mayor a 81%. Entonces:

$$0.81 < 1 - \frac{(W/L)_9}{(W/L)_{16}(r_{16} \parallel r_{17}) g_{m18} \beta} \tag{3.44}$$

$$\frac{(W/L)_9}{(W/L)_{16}(r_{16} \parallel r_{17}) g_{m18} \beta} < 0.19 \tag{3.45}$$

En base al análisis desarrollado en la presente sección se definieron los factores de forma de los transistores que conforman el circuito de protección. A continuación, se presentan las dimensiones de los transistores de cada uno de los bloques en los cuales se divide el circuito, así como los parámetros de los demás elementos del circuito.

Tabla 3.1: Factores de forma de los transistores que conforman el sensor de corriente.

Transistor	Tipo	W/L	W (um)	L (um)
M1	N	0.4	2	5
M2	P	10	10	1
M3	N	240	240	1
M4	N	20	100	5
M5	P	10	10	1
M6	N	240	240	1
M7	P	3000	6000	2
M8	P	30	60	2

Tabla 3.2: Factores de forma de los transistores que conforman el amplificador de transimpedancia.

Transistor	Tipo	W/L	W(um)	L(um)
M9	P	20	20	1
M10	N	180	180	1
M11	P	40	40	1
M12	N	60	60	1
M13	N	2	2	1
M14	P	30	30	1
M15	N	3.2	16	5
M16	P	130	130	1
M17	N	400	400	1

Tabla 3.3: Factores de forma del transistor que conforma el inyector de corriente.

Transistor	Tipo	W/L	W(um)	L(um)
M18	N	500	250	0.5

Tabla 3.4: Valores de otros componentes del circuito.

Componente	Nomenclatura	Valor
Resistencia	R	20KΩ
Voltaje de alimentación	VDD	3.3V
Voltaje de referencia	Vref	3V
Corriente de referencia	IR	10mA
Corriente de polarización	Iref	1uA

3.5 ELABORACIÓN DE LAYOUTS

En el flujo de diseño de un circuito integrado, la siguiente etapa corresponde a la elaboración del *layout* físico, el cual es la distribución de estructuras geométricas asociadas al circuito diseñado.

Estas estructuras son formadas por diversas capas de metal superpuestas una sobre otra. Algunas de estas capas se denominan polisilicio, metal 1, metal 2, difusión N+, difusión P+, etc. Cada una de estas presenta características definidas por el fabricante de circuitos integrados, de acuerdo a la tecnología sobra la cual este trabaje. La Figura 3.7 muestra un corte transversal de un circuito integrado donde se pueden distinguir las capas de metal anteriormente mencionadas.

A continuación, se describen los procesos de fabricación de un circuito integrado, reglas de diseño y técnicas involucradas en la elaboración de *layouts*.

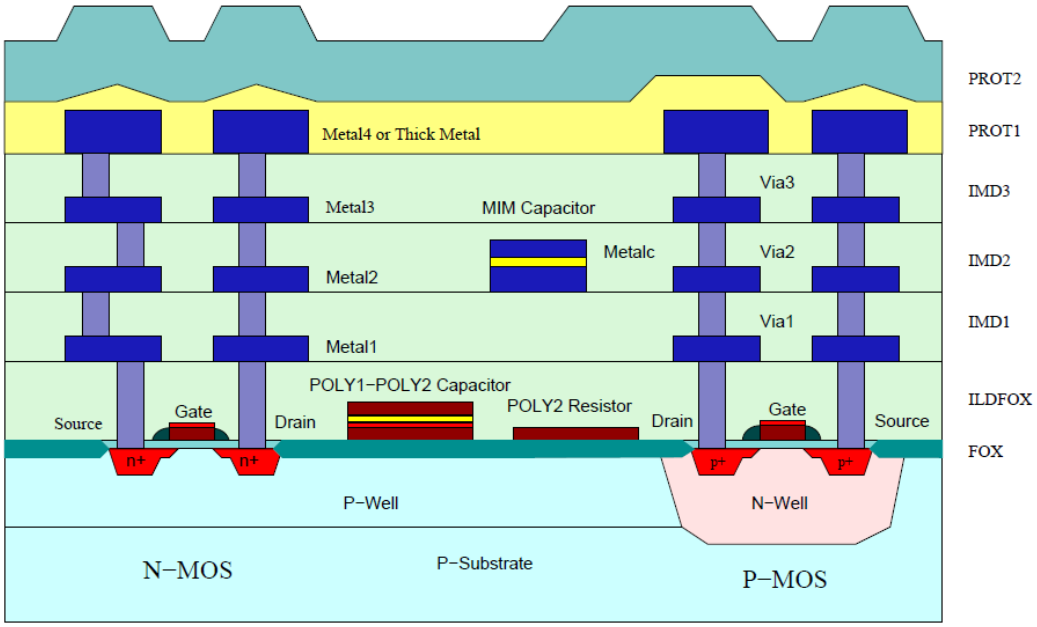

Figura 3.7: Distribución de capas de metal para la tecnología AMS 0.35um [23].

3.5.1 Procesos de fabricación

El material sobre el cual se construyen los circuitos integrados en la actualidad es el Silicio. Mediante el proceso de Czochralski se logra obtener un cristal de Silicio de forma cilíndrica

[5]. Esta estructura es cortada en finas capas, las cuales son denominadas obleas. Sobre esta oblea se realizan los siguientes procesos:

- Oxidación: Se realiza cuando se desea aislar a las diferentes pistas entre sí. Este proceso requiere la formación de óxido de Silicio. El espesor de esta capa define características funcionales del circuito integrado.

- Deposición: Su función principal es definir las pistas conductoras o aislantes. Se coloca sobre la oblea de Silicio una capa de polisilicio o aluminio, la cual es recortada de forma controlada por diversos métodos.

- Grabado: Se encarga de eliminar las zonas que no formarán parte de las pistas por medio de diversos métodos, como la litografía.

- Difusión: Permite el movimiento de átomos dentro de sólidos utilizando altas temperaturas. Se utiliza para dopar zonas específicas de la oblea de silicio.

- Implantación iónica: similar a la difusión, permite el dopado de zonas de la oblea pero con una mayor precisión por medio del bombardeo iónico.

3.5.2 Reglas de diseño

Cuando un diseñador de circuitos integrados desea implementar un determinado sistema, recurre a las reglas de diseño que le brinda el fabricante con el cual desea trabajar. Estas reglas toman en cuenta las diferentes variables que se presentan durante la fabricación del circuito y las limitaciones del proceso.

En la presente tesis se trabajará con la tecnología AMS 0.35 μm, desarrollada por la empresa Austriamicrosystem, la cual determina que la longitud mínima de canal en un transistor es de 0.35 μm y utiliza cuatro capas de metal. Esta empresa brinda a los usuarios documentos en donde se indican las reglas de diseño que estos deben tener en cuenta al momento de trabajar con la tecnología que ellos ofrecen [24]. Asimismo, informa a los usuarios sobre las limitaciones que se presentan al momento de fabricar un circuito integrado, las cuales se resumen en el documento de parámetros de proceso [25].

Al momento de realizar el *layout* de un circuito integrado, las principales reglas de diseño que se deben tener en cuenta son las siguientes:

- Distancia mínima entre pistas
- Tamaño mínimo de las pistas
- Distancia mínima entre metales y polisilio
- Desbordamiento entre pistas
- Solapamiento mínimo

3.5.3 Técnicas para la elaboración de *layouts*

Interdigitación

Cuando en el circuito diseñado se presenta un transistor con gran ancho de canal, este debe ser implementado usando la técnica de interdigitación. Un transistor con esta característica requiere de una gran área en sus terminales drenador y surtidor. Esto generará que la resistencia en estas zonas aumente y esto se traduce en el aumento de ruido del dispositivo. La técnica de interdigitación permite que la resistencia en el drenador y surtidor de transistores con un gran ancho de canal disminuya, a partir del uso de transistores de menor tamaño conectados en paralelo.

Simetría

Esta técnica es muy utilizada para poder implementar dispositivos que necesiten transistores idénticos en su estructura. Ejemplos de estos casos son los pares diferenciales y los espejos de corriente. Como criterio general, la distribución de transistores en un *layout* debe ser simétrica para poder reducir variaciones de proceso.

Gradiente

El gradiente hace referencia a las desigualdades de dopaje que se presentan en el *layout* luego de la implantación iónica. Esta proporciona características eléctricas diferentes a transistores que fueron diseñados tomando en cuenta características similares.

Esta técnica tiene como objetivo la disminución de los denominados gradientes para que los transistores sobre la oblea de silicio presenten las mismas cantidades de dopaje en su estructura.

CAPÍTULO 4

SIMULACIONES Y RESULTADOS

4.1 INTRODUCCIÓN

En el presente capítulo, se muestran las simulaciones que permiten verificar el funcionamiento del circuito de protección. Asimismo, se presenta el *layout* físico correspondiente, el cual se desarrolló con la herramienta LayoutXL.

4.2 SIMULACIONES

Las simulaciones de funcionamiento del circuito de protección se realizaron mediante la herramienta Virtuoso, el cual usa el simulador Spectre. El modelo de transistor MOS que utiliza este simulador es el BSIM3v3.

En primer lugar, se realizaron simulaciones al sensor de corriente. Se realizó un análisis transitorio y se observó el comportamiento de la señal V_{DD-C} en el tiempo. La Figura 4.1 muestra la gráfica otorgada por el simulador Spectre. El microprocesador criptográfico es modelado como la suma de varias corrientes con frecuencias entre $1MHz$ y $5MHz$. Estos

presentan un rango de corrientes entre $2mA$ y $8mA$. Se fijó el voltaje de referencia $V_{REF} = 3V$ y la corriente $I_{REF} = 1\mu A$ con una fuente de voltaje ideal y una fuente de corriente ideal, respectivamente. En base al resultado obtenido, se verifica que el sensor de corriente logra mantener el voltaje V_{DD-C} cercano a $3V$ pese a las variaciones de consumo que presenta el microprocesador.

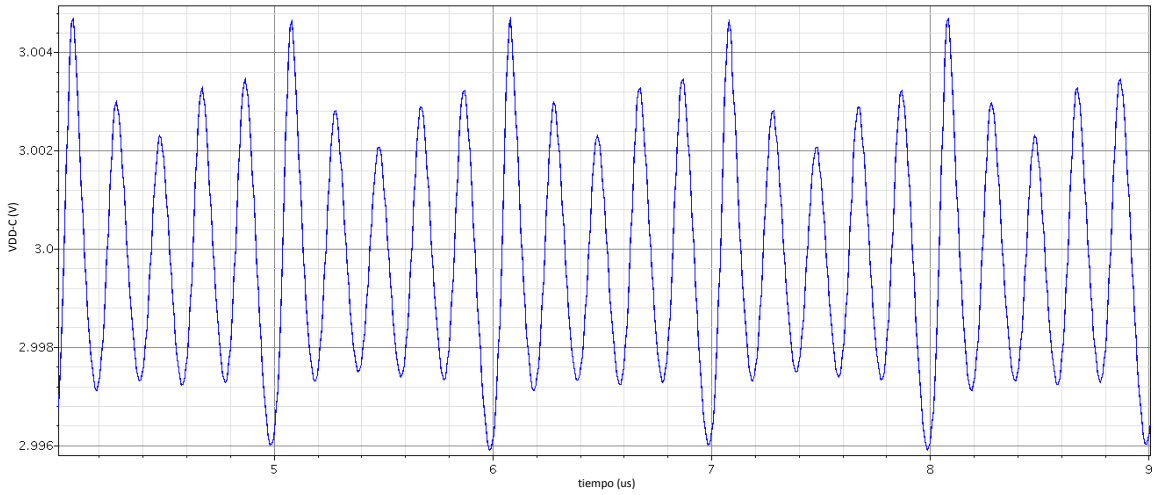

Figura 4.1: Señal de voltaje V_{DD-C}

En los capítulos anteriores, se mencionó que el sensor de corriente tiene como objetivo copiar la corriente consumida por el procesador de la tarjeta inteligente con un factor $\beta = 0.01$. La Tabla 4.1 muestra el punto de operación de los transistores $M7$ y $M8$. Se puede observar que la corriente es copiada de manera satisfactoria.

Tabla 4.1: Parámetros obtenidos en la simulación del espejo de corriente.

Transistor	Id (uA)	gm (uS)	VGS (mV)	VDS (mV)	VDsat (mV)
M7	10002.3	4160	1091	349.4	366.7
M8	104.5	508	1091	1253	366.7

Para verificar la respuesta en frecuencia del sensor de corriente se realizó un análisis AC. El resultado se muestra en la Figura 4.2. Se puede establecer que el margen de fase es de $45°$, lo cual indica que este bloque es estable. Asimismo, este presenta un ancho de banda de $42MHz$. Esto muestra que el circuito cumple con el requerimiento de poseer un ancho de banda mayor a $5MHz$. Este bloque otorga una atenuación de $24.3dB$.

La Tabla 4.2 muestra los parámetros obtenidos en la simulación del amplificador diferencial de carga activa. Todos los transistores trabajan en la región de saturación y logran que circulen las corrientes esperadas.

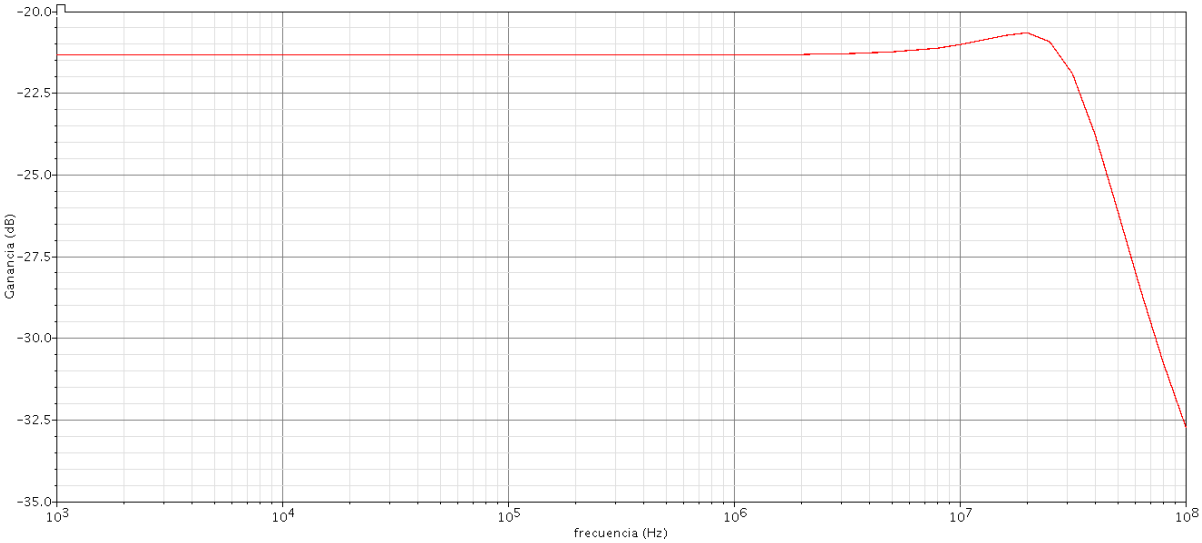

Figura 4.2: Respuesta en frecuencia del sensor de corriente.

Tabla 4.2: Parámetros obtenidos en la simulación del amplificador diferencial con carga activa.

Transistor	Id (uA)	gm (uS)	VGS (mV)	VDS (mV)	VDSsat (mV)
M1	1	9.51	689.3	689.3	145.1
M2	25.43	144	1053	1053	318
M3	25.43	595.4	973.4	221.1	55.04
M4	50.9	9.638	689.3	2026	145.1
M5	25.48	144.3	1053	1091	318
M6	25.48	595.5	973.7	182.8	55.15

Posteriormente, se realizaron simulaciones al amplificador de transimpedancia. La Tabla 4.3 muestra el resultado del análisis DC que se realizó. Se verifica que todos los transistores trabajan en la región de saturación.

Tabla 4.3: Parámetros obtenidos en la simulación del amplificador de transimpedancia.

Transistor	Id (uA)	gm (uS)	VGS (mV)	VDS (mV)	VDSsat (mV)
M9	83.84	363.2	1148	1148	403.2
M10	83.84	1409	1053	104.6	88.01
M11	88.36	546.8	1258	1380	314.7
M12	88.36	1080	666.9	666.9	116.7
M13	10.02	65.98	1226	1226	234.1
M14	10.02	143.6	1085	1085	139.2
M15	10.02	9.523	689.3	788.8	145.1
M16	535.9	2308	1148	2358	406.9
M17	535.9	6541	666.9	941.6	116.7

La respuesta en frecuencia del amplificador se realizó por medio de un análisis AC. La corriente de error fue simulada como una fuente de corriente alterna de $1A$ de amplitud. En la Figura 4.3 se muestra el resultado obtenido. Se determina que su ancho de banda es de $2.3MHz$ y su ganancia es de $108dB$.

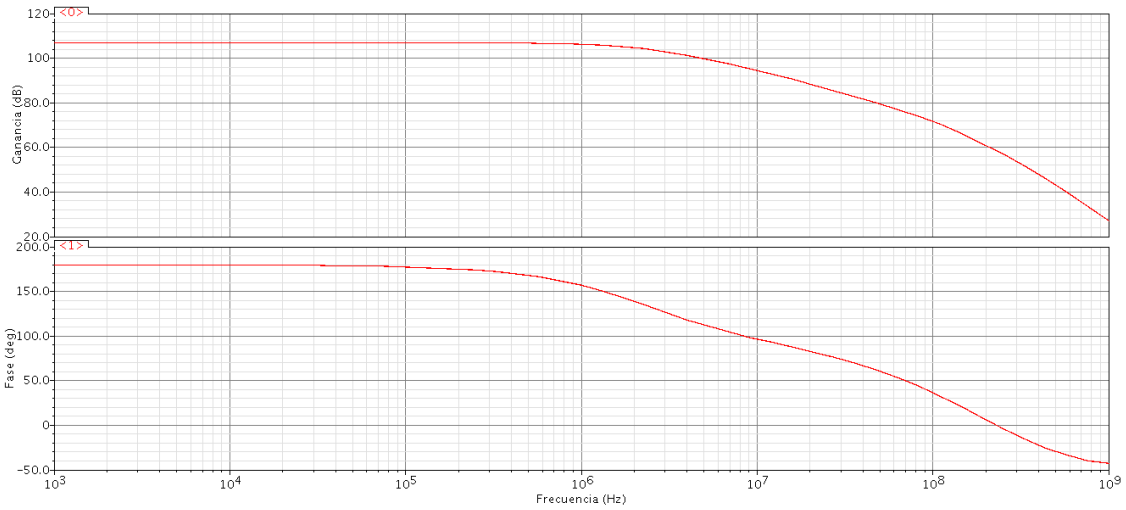

Figura 4.3: Respuesta en frecuencia del amplificador de transimpedancia.

El punto de operación del inyector de corriente se presenta en la Tabla 4.4. Se observa que su punto de operación coincide con el nivel DC elegido para el microprocesador criptográfico.

Tabla 4.4: Parámetros obtenidos en la simulación del inyector de corriente.

Transistor	Id (uA)	gm (uS)	VGS (mV)	VDS (mV)	VDSsat (mV)
M18	4972	22160	941.6	3000	274.6

A continuación, se realizó un análisis AC al lazo de control. El resultado se muestra en la Figura 4.4. Se determina que el circuito de protección presenta un margen de fase de $35°$, ancho de banda de $80MHz$. Asimismo, se verifica que el circuito funciona correctamente ya que logra $17dB$ de atenuación.

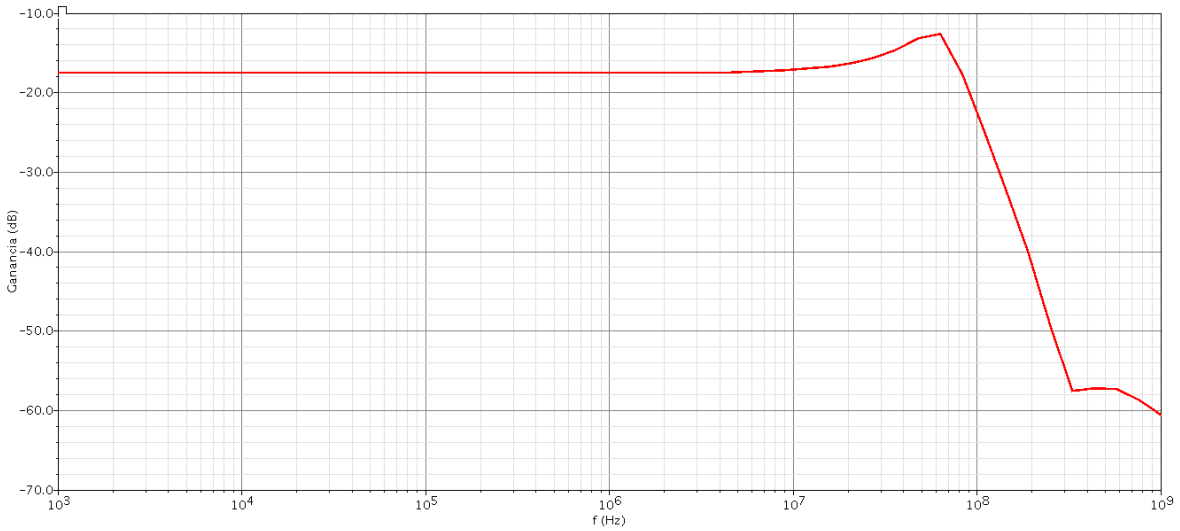

Figura 4.4: Respuesta en frecuencia del circuito de protección.

Finalmente, se realizó una simulación transitoria para observar el comportamiento de las corrientes de interés dentro del circuito.

En la Figura 4.5 se muestran las corrientes consumidas por el microprocesador (I_M) y la corriente vista desde la fuente de alimentación (I_{DD}). Para esta simulación, el microprocesador fue modelado como varias fuentes de corrientes en paralelo, cada una de ellas con diferentes valores de amplitud y frecuencia. De esta manera se emula la señal de corriente consumida por el microprocesador durante una operación criptográfica. Se determina que la corriente I_{DD} es cercana a $10mA$, y que el valor de atenuación es de 86%.

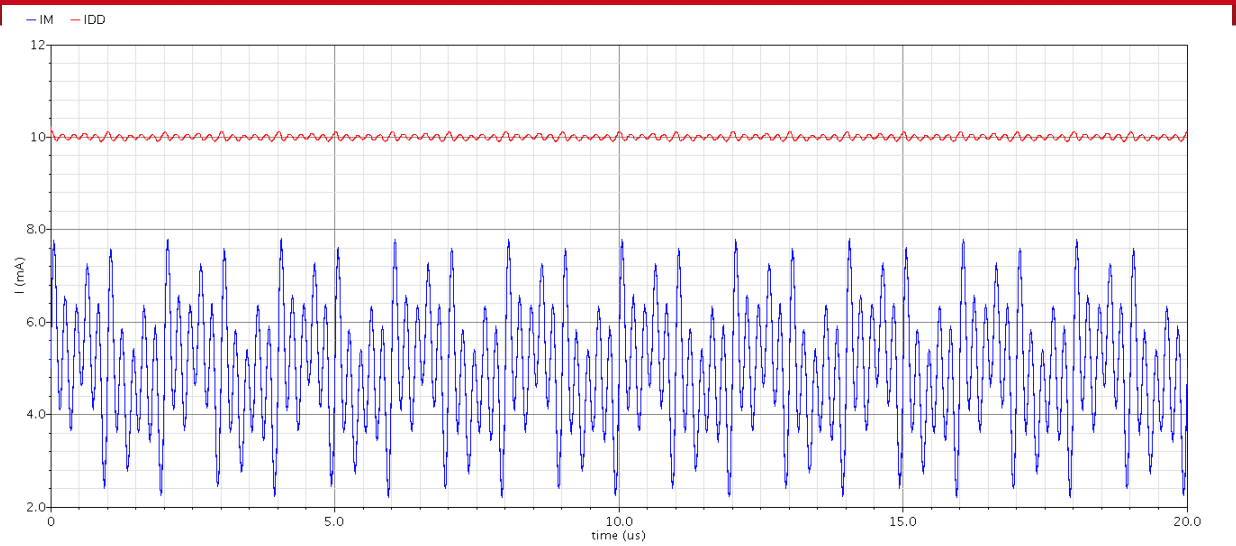

Figura 4.5: Respuesta en el tiempo del circuito de protección.

En base al porcentaje de atenuación logrado, se puede determinar el valor de NTC-DPA obtenido con el circuito diseñado. Se determina que:

$$NTC - DPA = 1100$$

Este resultado nos muestra que el circuito diseñado es capaz de dificultar el éxito de un ataque DPA en tarjetas inteligentes.

4.3 LAYOUT DEL CIRCUITO DE PROTECCIÓN

En primer lugar, fue necesario realizar el circuito esquemático del circuito total, el cual se muestra en la Figura 4.6. Este contiene información acerca de las características físicas de cada uno de los transistores y se desarrolló usando la herramienta Virtuoso. Una de las características de esta herramienta es que permite definir el tipo de técnica que se desea usar en el *layout* físico. Principalmente, se utilizó la técnica de interdigitación ya que se emplean varios espejos de corriente. De esta manera, se reducen variaciones indeseadas en las características físicas de los transistores.

Luego de obtener los resultados mostrados anteriormente, se procedió a elaborar el *layout* físico del circuito de protección. En la Figura 4.7 se muestra dicho *layout*, el cual fue elaborado con la herramienta LayoutXL. Se pueden distinguir los tres bloques principales del circuito, así como los terminales del circuito. El área total ocupada por el circuito de protección es igual a $60000\,\mu m^2$.

4.4 RESUMEN Y COMPARACIÓN DE RESULTADOS

En la Tabla 4.5 se puede apreciar los principales parámetros de los trabajos mostrados en [7], [8] y [9]. Finalmente se presentan los resultados obtenidos en el presente trabajo.

Tabla 4.5: Comparación del presente trabajo con trabajos similares.

Diseño	Atenuación de corriente (%)	Área ocupada (um2)	Potencia consumida (mW)	Tecnología CMOS (um)	Voltaje de alimentación (V)	Corriente de referencia (mA)
Ref. [7]	95	13000	18.94	0.18	1.8	10
Ref. [8]	90	57600	-	0.18	1.8	5
Ref.[9]	-	-	41	0.18	3.3	12
Diseño propuesto	86	60000	35.5	0.35	3.3	10

Cabe resaltar que los valores obtenidos de los trabajos anteriores son valores medidos en circuitos fabricados, mientras que los valores obtenidos a partir de nuestro estudio son valores provenientes de simulaciones.

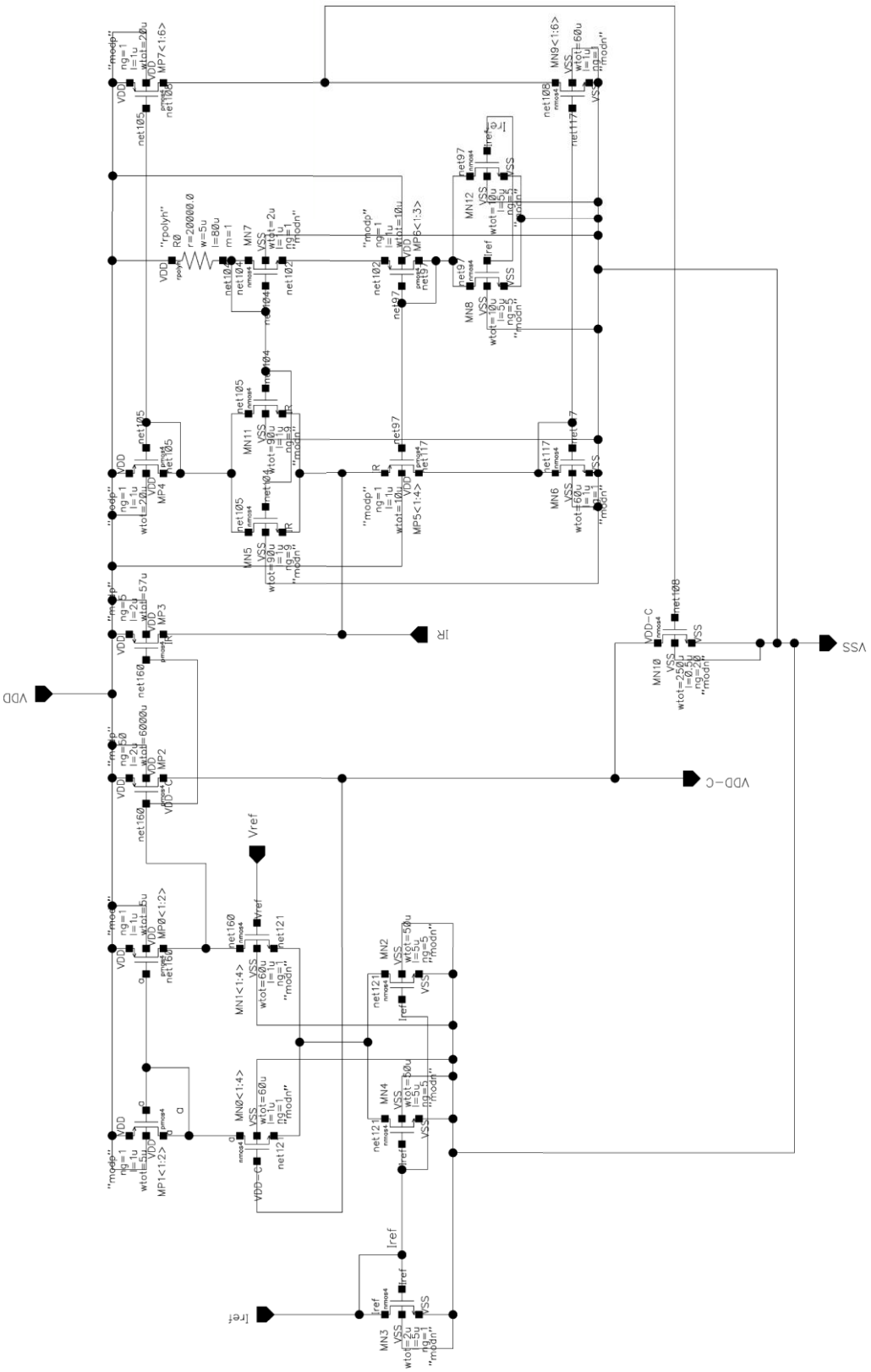

Figura 4.6: Diagrama esquemático desarrollado con la herramienta Analog Environment.

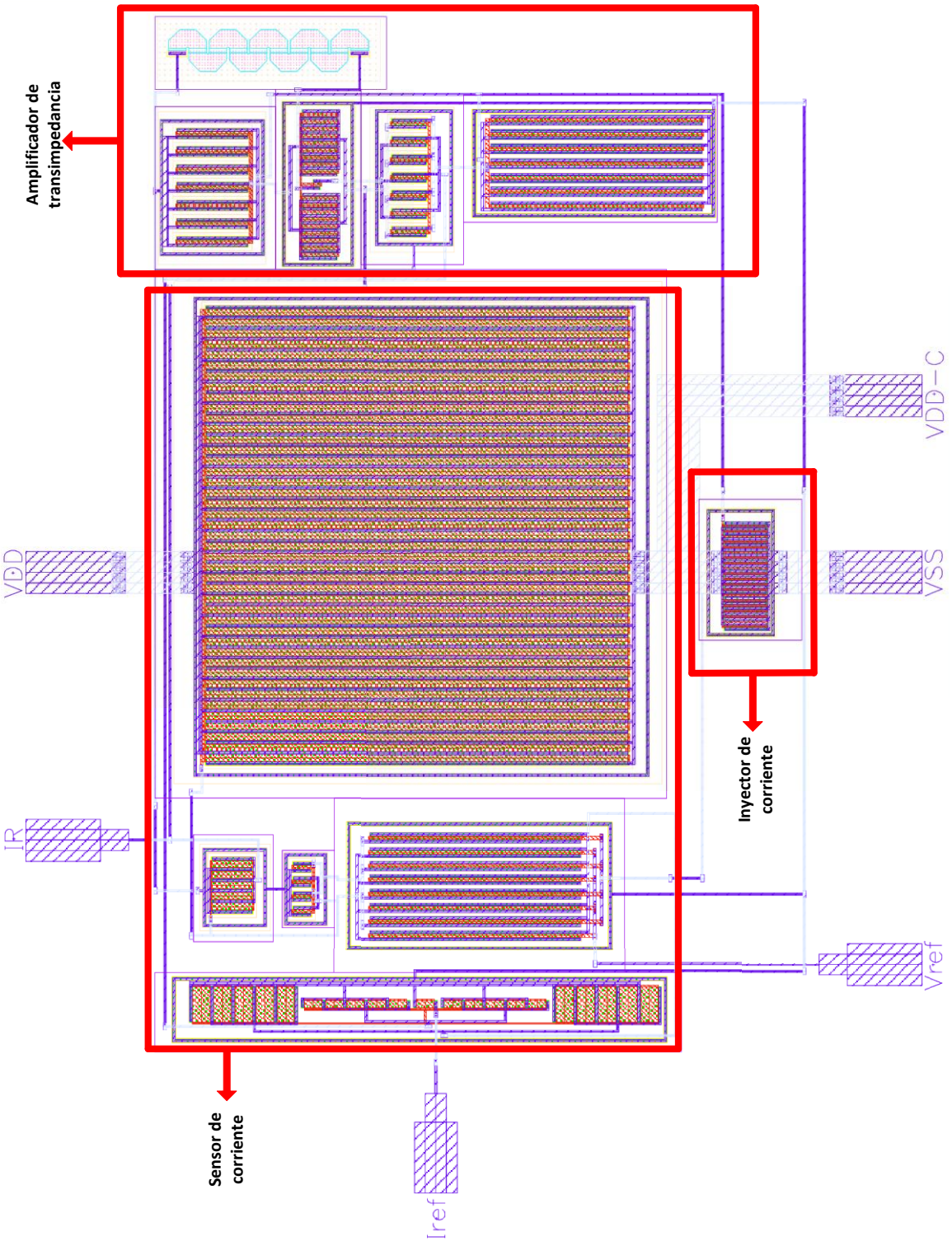

Figura 4.7: Layout del circuito de protección desarrollado con la herramienta LayoutXL.

CONCLUSIONES

- Se concluye que la técnica denominada Atenuación de corriente, basada en la atenuación de variaciones de consumo de corriente en una tarjeta inteligente, es una solución ante los ataques DPA.

- El circuito de protección diseñado logra una atenuación de variaciones de consumo de corriente igual a 86%. De esta manera, se cumple con el requerimiento necesario para proteger a las tarjetas inteligentes de Clase B ante ataques DPA. El NTC-DPA logrado es igual a 1100 muestras, lo cual muestra la robustez del circuito.

- El funcionamiento del circuito diseñado es independiente de las capacidades del microprocesador y del algoritmo criptográfico del dispositivo a proteger. Es por ello que puede ser utilizado como un dispositivo de propósito general de seguridad ante ataques DPA.

RECOMENDACIONES

- Se pudo observar durante el diseño del circuito que, a medida que se eleva la corriente de referencia, la respuesta del circuito mejora y se incrementa el porcentaje de atenuación, tal como se menciona en [9]. Sin embargo, el valor de la corriente de referencia está limitada con el consumo de potencia máximo establecido en los requerimientos del circuito.

- En la presente tesis no se tomó en cuenta el diseño de las fuentes de referencia necesarias para el funcionamiento del circuito. Estas deben ser diseñadas para lograr que este sea capaz de ser implantado en una tarjeta inteligente.

- Para la implementación sobre la tarjeta inteligente, es importante que el circuito cuente con diodos de protección para evitar descargas electroestáticas.

- Se recomienda que el circuito de protección sea segmentado en bloques más pequeños y dispersado alrededor del microprocesador para su implementación en la tarjeta inteligente. De esta manera, se protege al dispositivo contra un posible ataque electromagnético.

- Se recomienda realizar simulaciones post-layout para tener resultados que tomen en cuenta las características parásitas propias del *layout* físico.

BIBLIOGRAFÍA

[1] W. Rankl, W. Effing
2002 "Smart Card Handbook", tercera edición

[2] B. Razavi
2001 "Design of Analog CMOS Integrated Circuits", McGraw-Hill

[3] Y. Tsividis
1999 "*Operation and Modeling of the MOS transistor*", 2nd ed. McGraw-Hill

[4] C. Saint, J, Saint
2002 "IC Mask Design", McGraw-Hill

[5] A. Hastings
2001 "The Art of Analog Layout", Prentice Hall

[6] P. Kocher, J. Jaffe, B. Jun
1999 "*Differential Power Analysis"*, Cryptography Research, Inc., Springer-Verlag, pp. 388-397

[7] H. Vahedi, S. Gregori, R. Muresan
2011 "*The effectiveness of a current flattening circuit as countermeasure against DPA attacks"*, Microelectronics Journal, volume 42, issue 1, pages 180-187

[8] H. Vahedi, R. Muresan, S. Gregori
2006 "On-Chip Current Flattening Circuit with Voltage Scaling", Proc. IEEE Int'l Symp. Circuits and Systems (ISCAS '06) pp. 4277-4280

[9] R. Muresan, S. Gregori
2008 "Protection circuit against Differential Power Analysis Attacks for Smart Cards", IEEE Trans. Comput., vol. 57, pp. 1540-1549

[10] H. Hernandez, J. Scott, W. Van Noije
2012 "DPA insensitive voltage regulator for contact smart cards", Universidad de Sao Paulo

[11] H. Vahedi, R. Muresan, S. Gregori
2009 "On-Chip power efficient Current Flattening Circuit", Journal of Circuits and Systems and Computers 18, pp. 565-579

[12] K. Rabah, "Theory and implementation of data encryption standard: A review", Information Technology Journal, 4: 307-325

[13] C. Jie, Z. Qiang, D. Guoliang, D. Gaoming
2007 "Differential Power Analysis for Cryptographic ICs", IEEE

[14] G. Ratanpal, R.Williams, T. Blalock
2004 "An On-Chip Signal Suppression Countermeasure to Power Analysis Attacks", IEEE

[15] S. Soydan
2010 "Analyzing the DPA Leakage of the Masked S-box via Digital Simulation and Reducing the Leakage by Inserting Delay Cells", IEEE

[16] A. Zadali, A. Golabpour, M. Doostari, M. Broujerdian
2008 "Differential Power Analysis in the Smart card by Data simulation", IEEE

[17] H. Vahedi, R. Muresan, S. Gregori
2013 "Design of Secure Microsystems Using Current-to-Data Dependence Analysis", Scientific Research

[18] J. Zhang, D. Gu, Z. Guo, L. Zhang
2010 "Differential Power Cryptanalysis Attacks against PRESENT Implementation", IEEE

[19] J. Ambrose, N. Aldon, A. Ignjatovic, S. Parameswaran
2008 "Anatomy of Differential Power Analysis for AES", IEEE

[20] ISO/IEC 7816-3
2006 "Identification cards – Integrated circuit cards / Part 3: Cards with contacts – Electrical interface and transmission protocols", tercera edición

[21] A. Sison, B. Gerardo, B. Tanguilig III, Y. Byun
2011 "An improved Data Encryption Standard to Secure Data using Smart Cards", IEEE

[22] H. Mahnoud, K. Alghathbar
2010 "Novel Algorithmic Countermeasure for Differential Power Analysis Attacks on Smart Cards", IEEE

[23] Austriamicrosystems
2008 "0.35um CMOS C35 Process parameters", revision #6.0

[24] Austriamicrosystems
2011 "0.35um CMOS C35 Design rules", revision #9.0

[25] Austriamicrosystems
2009 "0.35um CMOS C35 Matching parameters", revision #3.0