

Universidad de Costa Rica
Facultad de Ingeniería
Escuela de Ingeniería Eléctrica

Implementación en Verilog de Unidad de Generacion de Rayos para GPU Theia.

Por:

Josué David Vargas Amador

Ciudad Universitaria “Rodrigo Facio”, Costa Rica

Diciembre de 2015

Implementación en Verilog de Unidad de Generacion de Rayos para GPU Theia.

Por:

Josué David Vargas Amador

IE-0499 Proyecto eléctrico

Aprobado por el Tribunal:

MSc. Diego Valverde Garro
Profesor guía

MSc. Carlos Duarte Martínez
Profesor lector

MSc. Rodolfo Brenes Fernández
Profesor lector

Índice general

Índice de figuras	vi
Índice de tablas	vii
1 Introducción	1
1.1 Justificación	1
1.2 Alcances del proyecto	2
1.3 Objetivos	2
1.4 Metodología	2
1.5 Desarrollo	3
2 Marco Teórico	5
2.1 GPU	5
2.2 Raycasting	5
2.3 Arquitecturas con unidades de generación de rayos	7
2.4 Arquitectura de TheiaV3	8
2.5 Métodos de normalización	9
2.6 Punto fijo sin signo	10
2.7 Verificación funcional	11
3 Desarrollo de la aplicación	13
3.1 Generalidades	13
3.2 Operaciones con el método de Newton Raphson	14
3.3 Consideraciones del Punto Fijo	14
3.4 Estructura del RGU	15
3.5 Instrucciones de iteración	15

Índice de figuras

Índice de tablas

1 Introducción

1.1 Justificación

Los sistemas computacionales actuales poseen, dentro de su arquitectura, módulos de hardware especializados llamados Unidades de Procesamiento Gráfico (GPU, por sus siglas en inglés) encargados de acelerar el proceso de representación de objetos tridimensionales en la pantalla del computador.

Las unidades de procesamiento gráfico permiten la visualización de objetos mediante el cálculo de las primitivas que conforman el modelo abstracto de las imágenes. Las GPU implementan distintos algoritmos de representación gráfica, entre estos, uno es el algoritmo de Ray Casting.

El algoritmo de Ray Casting genera vectores (rayos) normalizados desde la perspectiva del usuario y calcula la intersección de los rayos con los objetos del escenario, además colabora con la formación de los colores, con la finalidad de crear las imágenes mostradas en pantalla.

Entonces los cálculos para la representación de objetos visuales en una GPU de tipo raycasting requieren de una arquitectura interna capaz de la generación de vectores (rayos) normalizados, para luego usar estas estructuras de datos en los módulos dedicados a la intersección de rayos. La generación de rayos requiere de instrucciones capaces de realizar cálculos aritméticos como multiplicaciones, sumas y restas, así como operaciones especializadas que permitan aproximar los valores de raíces cuadradas, por lo que el diseño lógico de una unidad dedicada facilitaría el proceso de creación rayos y permitiría añadir flexibilidad y modularidad al diseño de todo el GPU. Existen proyectos de hardware relacionados al diseño de arquitecturas de trazado de rayos que implementan unidades de generación de rayos propias como SaarCor de la Universidad de Saarland (?) y RayCore de la Universidad de Sejong (?).

En el caso de la GPU de tipo raycasting Theia, las especificaciones arquitectónicas indican la necesidad de una Unidad de Generación de Rayos (RGU, por sus siglas en inglés). La RGU debe poseer un conjunto de instrucciones necesarias para el cálculo de la normalización de vectores tridimensionales empleados en las siguientes etapas de funcionamiento del GPU.

1.2 Alcances del proyecto

La GPU Theia se encuentra en su tercera iteración, y en esta etapa tiene dos módulos principales dentro de su descripción de RTL en el lenguaje Verilog: la unidad de generación de rayos normalizados (RGU) y el módulo de intersección de rayos de tipo AABB (siglas en inglés de Axis Aligned Bounding Boxes).

El módulo de la RGU es un módulo que posee dentro de su descripción las instrucciones necesarias para el funcionamiento apropiado de la generación de rayos normalizados. Estas instrucciones deben ser capaces de proveer la información necesaria para programar el módulo de la RGU de manera que permita la normalización de los vectores mediante cálculo aproximado del inverso de la raíz cuadrada empleando el método iterativo para aproximación de raíces Newton-Raphson.

Posterior a esto se debe plantear un ambiente de verificación funcional que permita afirmar que el módulo RGU está cumpliendo con su papel dentro de la arquitectura y que puede generar la información requerida por los módulos de intersección de rayos.

1.3 Objetivos

Objetivo general

Desarrollar el modelo por comportamiento en Verilog de una Unidad de Generación de Rayos de un GPU tipo ray casting.

Objetivos específicos

Desarrollar el modelo por comportamiento en Verilog de una Unidad de Generación de Rayos de un GPU tipo ray casting.

- Investigar bibliografía sobre el mecanismo generación de rayos.
- Definir el mecanismo de generación de rayos normalizados en el GPU.
- Verificar el comportamiento funcional de la Unidad de Generación de Rayos en el GPU.

1.4 Metodología

1. Se procederá a investigar los conceptos fundamentales de la arquitectura de la GPU, el algoritmo de ray casting y sobre los posibles mecanismos de la generación de rayos normalizados.

2. Se buscará la implementación final de la arquitectura interna de la RGU de modo que contenga las instrucciones necesarias para la normalización.
3. Se simulará la ejecución del código en la RGU para generar los rayos normalizados necesitados por los módulos de intersección de rayos de tipo AABB.
4. Se verificará el comportamiento funcional del módulo RGU con la finalidad de establecer un marco de referencia para la futura validación del resto de la versión actual del GPU Theia.

1.5 Desarrollo

Este proyecto se estructura por medio de capítulos, cada uno tiene como tarea aclarar los siguientes tópicos:

1. Capítulo I: Introducción. Muestra la justificación del proyecto, los alcances y limitaciones, los objetivos y la metodología que permite cumplir los mismos.
2. Capítulo II: Antecedentes y Marco Teórico. Introduce al lector conceptos claves de arquitectura de unidades de procesamiento gráfico, algoritmo de raycasting, y plantea los casos de proyectos donde se han implementado chips.
3. Capítulo III: Implementación final de la unidad de generación de rayos. Aquí se describe la arquitectura final de la unidad, así como el método empleado usando las instrucciones de ésta para implementar la unidad.
4. Capítulo IV: Prueba de verificación funcional. Se comprueba la funcionalidad del módulo conductual de lenguaje Verilog por medio de un ambiente de verificación apropiado.
5. Capítulo V: Conclusiones y recomendaciones. Se muestran posibles resultados del proyecto y reflexiones sobre el futuro del proyecto.

2 Marco Teórico

2.1 GPU

Definición

Las unidades de procesamiento gráfico se encargan de rápidamente renderizar (representar) objetos 3D en forma de píxeles en la pantalla de la computadora, típicamente, por medio de arquitecturas de hardware basadas en la técnica de rasterización. La mayor parte de las GPU han sido diseñadas para realizar operaciones fijas organizadas en forma de pipeline para ir pasando vértices y píxeles a través de distintas etapas.

A continuación se mencionan las etapas principales del pipeline de gráficos:

1. El programa de usuario proporciona los datos al GPU en la forma de primitivas como puntos, líneas y polígonos que describen la geometría 3D.
2. Etapa geométrica: las primitivas geométricas son procesadas en base a los vértices y son transformados de coordenadas 3D a triángulos 2D en la pantalla..
3. Etapa de rasterización: en esta etapa se dibuja una imagen mediante el uso de los datos anteriormente generados así como de los cálculos computacionales por píxel. La salida es un conjunto de píxeles donde cada píxel posee sus propios atributos (color, sombras, etc).

Los conjuntos de datos muy grandes que deben ser visualizados en tres dimensiones normalmente son creados usando representaciones de superficies mediante el dibujo de primitivas geométricas que crean mallas poligonales (en la mayoría de casos son mallas triangulares), pero las técnicas convencionales al usarse en el renderizado de datos volumétricos producen pérdidas en la visualización. Las técnicas de renderización de volumen tienen más información que los métodos de renderización por superficie pero poseen una mayor complejidad y mayores tiempos de renderización.

2.2 Raycasting

Se presentan detalles acerca del algoritmo de raycasting en el cual se basa el GPU Theia para su funcionamiento.

Definición

El algoritmo de raycasting funciona haciendo cálculos a un píxel a la vez, y para cada píxel la tarea básica es encontrar el objeto que es observado en la posición correspondiente a ese píxel en la imagen, o sea parte del observador hacia los objetos a visualizar contrario al método por rasterización. Se puede decir que cada píxel ve en una dirección distinta y cualquier objeto que es observado por un píxel debe intersectar el rayo proveniente desde el punto de vista de la cámara. El objeto esperado es aquel que es intersectado primero por el rayo más cercano a la cámara. Una vez que el objeto es encontrado, se emplea el punto de intersección, la superficie normal, y alguna otra información del objeto para definir el color de cada píxel.

Entonces se puede decir que un algoritmo de raycasting tiene tres partes básicas:

1. Generación de rayo: donde se calcula el origen y la dirección de cada rayo (vector) del píxel correspondiente en la vista de la cámara.
2. Intersección de rayo: donde se determina el objeto más cercano en la intersección del rayo proveniente de la cámara.
3. Shading: donde se calcula el color del píxel basado en los resultados de la intersección de rayos.

Con el objetivo de generar rayos, primero se necesita una representación matemática de un rayo. Un rayo en realidad es solo un punto de origen y una dirección propagación, una línea paramétrica en 3D que va desde el ojo llamado punto e hasta otro punto s que está en el plano de la imagen está dada por:

$$p(t) = e + t(s - e) \quad (2.1)$$

Esta fórmula implica que se empieza en el punto e y se avanza a través del vector $s-e$ hasta llegar al punto p . Valores negativos de t implica que se encuentra el rayo detrás del ojo.

Un pseudocódigo sobre el algoritmo de raycasting se muestra se muestra abajo en el pseudocódigo 2.

En términos generales se puede afirmar que la técnica de raycasting evalúa el color de cada pixel en la imagen al disparar un rayo a través de la escena desde la posición del observador. Si el rayo golpea el volumen, el color del pixel es calculado muestreando los datos a lo largo del rayo en un número finito de posiciones en el volumen y combinando cada resultado en uno solo. Este método tiene una limitación al ejecutarse en los CPUs: para volúmenes de datos grandes el tiempo de renderización para una sola imagen es muy alto para visualización en tiempo real.

Algorithm 1 Algoritmo de Raycasting

```

1: procedure RAY-CAST
2:   for do cada pixel
3:     Construya un rayo desde el ojo
4:     for do para cada objeto en la escena
5:       Encuentre la intersección con el rayo
6:       Guarde esta intersección si es la más cercana

```

Transformaciones**2.3 Arquitecturas con unidades de generación de rayos**

Existen en la literatura pocas referencias a unidades de raycasting o de ray tracing (variante del algoritmo de ray casting que genera rayos secundarios por medio de la recursión en el punto de incidencia del rayo original) que mencionen explícitamente dentro de su arquitectura la implementación de unidades de generación de rayos, las principales referencias son dos proyectos de hardware provenientes de la Universidad de Saarland: SaarCOR y DRPU. En los artículos no se mencionan detalles de cómo se implementaron unidades de generación de rayos, solo se hablan de ellas de forma muy general.

SaarCOR

SaarCOR es el nombre de la unidad de ray tracing que fue diseñado para un chip de uso específico que está conectado por medio de un sistema de bus "host"(huésped) a otros chips que están en la misma placa de computadora. SaarCOR está dividido en tres unidades principales: la unidad de generación de rayos y de "shading"(RGS), el núcleo de ray tracing (RTC) y una unidad de manejo de acceso a memoria (RTC-MI).

DRPU

DRPU es el diseño y la implementación de un ASIC para procesamiento de ray tracing que posee capacidades de programabilidad similares a un GPU convencional en la universidad de Saarland. La arquitectura consiste en dos partes principales: Unidades de Ray Casting (encargadas de las estructuras espaciales) y un Procesador de "Shading"(encargado de hacer labores de sombreado y de generación de rayos).

RayCore

RayCore es el diseño y la implementación de una unidad de ray tracing para dispositivos móviles y de bajo consumo por parte de miembros de la Universidad de Sejong en Corea del Sur. Dentro de RayCore existen dos unidades principales: una Unidad de Creación de Árboles (TBU) y una Unidad de Ray-Tracing (RTU). Dentro de RTU hay una unidad de generación de rayos tanto primarios como secundarios definidos por la unidad Set-Up y por la unidad de "shading", respectivamente.

2.4 Arquitectura de TheiaV3

Introducción a TheiaV3

TheiaV3 es la tercera iteración del GPU multinúcleo de tipo raycasting Theia. El proyecto Theia es un proyecto de la modalidad Open Source (Código Libre) para experimentar con el hardware gráfico 3D.

El principal objetivo del proyecto Theia es proveer un ambiente Open Source incluyendo un código RTL funcional, un ambiente de pruebas y un lenguaje libre de alto nivel y un compilador para programar a Theia.

El hardware de Theia es descrito usando código RTL escrito en Verilog 2001. Para realizar una simulación completa del código RTL, se necesita tanto un conjunto de archivos para representar los parámetros de entrada, así como el código de usuario en representación binaria.

Descripción general del sistema

Theia es una unidad de procesamiento gráfico (GPU) multinúcleo, que se encuentra compuesto de distintos bloques que interactúan entre ellos con la finalidad de renderizar cuadros de imágenes.

En la figura se muestran los principales bloques funcionales de Theia así como la memoria principal que se encuentra en el exterior del GPU. La memoria principal es una memoria de tipo RAM que es empleada para almacenar las variables geométricas, el código, entre otros detalles.

Unidad de Generación de Rayos

La Unidad de Generación de Rayos (RGU por sus siglas en inglés) es un módulo de hardware encargado de la generación de las estructuras de datos que representan los rayos que son enviados a los otros módulos encargados de la intersección de los mismos. La RGU tiene un conjunto limitado de operaciones aritméticas así un conjunto de instrucciones propias orientadas a la generación de los rayos por lo que carece de instrucciones de control de flujo.

2.5 Métodos de normalización

La Unidad de Generación de Rayos de TheiaV3 debe realizar la operación del inverso de la raíz cuadrada con el objetivo de normalizar el rayo (vector) visto desde el observador, para lo cual se debe implementar dentro de la unidad un mecanismo que permita calcular una aproximación por medio de instrucciones aritméticas simples y de una forma rápida. A continuación se describen los métodos posibles.

Existen varios tipos de posibles algoritmos para el cálculo de raíces cuadradas pero en realidad para la implementación en microprocesadores hay pocos, y estos caben en dos categorías: multiplicativos y sustractivos. Los métodos multiplicativos normalmente se implementan en hardware junto con el multiplicador de la unidad de punto flotante y permite realizar operaciones rápidamente, y por otro los métodos sustractivos emplean hardware dedicado a estas operaciones, lo cual incrementa la latencia y los vuelve técnicas más lentas.

Métodos multiplicativos

Los algoritmos multiplicativos se suelen emplear para realizar cálculos estimados de raíces cuadradas usando iteraciones a partir de un estimado inicial. Emplear este tipo de técnicas reducen la ejecución de una operación de raíz cuadrada en una serie de multiplicaciones, sustracciones, y corrimientos de bits. Además vale la pena resaltar que estos métodos numéricos convergen cuadráticamente, lo cual implica que un estimado inicial apropiado preciso proporcionará resultados más precisos por cada iteración. Las técnicas empleadas frecuentemente en microprocesadores son los métodos de Newton-Raphson y de Goldschmidt, donde ambos métodos comparten muchos detalles en común pero se diferencian en el orden en que realizan las operaciones.

Newton-Raphson

El método de Newton-Raphson es un método iterativo de convergencia cuadrática que emplea multiplicaciones sucesivas para aprovechar las capacidades de multiplicación rápida de los procesadores contemporáneos.

Al ser Newton-Raphson un método plenamente iterativo, con el objetivo de reducir las iteraciones que se realizan en los cálculos se suele emplear tablas de hardware las cuales se emplean como punto de partida en el proceso de iteraciones.

El método de Newton-Raphson se fundamenta encontrar la mejor aproximación posible al valor de las raíces o ceros de una función $F(x)$ donde $F(x) = 0$.

Entonces mediante el método de Newton-Raphson si se inicia iterando a partir de un valor X_0 aproximado al valor deseado, entonces se tiene la expresión 2.2

$$\begin{aligned} f'(x_0) &= \frac{f(x_0)}{x_0 - x_1} \\ x_1 &= x_0 - \frac{f(x_0)}{f'(x_0)} \end{aligned} \quad (2.2)$$

Aplicando la definición del método de Newton-Raphson a la ecuación $x^{-2} - S = 0$ donde la raíz es $\frac{1}{\sqrt{S}}$ se obtiene la expresión (2.3):

$$R_{i+1} = R_i(3 - SR_i^2)/2 \quad (2.3)$$

donde S es el valor de la base de la raíz y R_i el valor del cálculo de la raíz cuadrada en la iteración i. El valor de la iteración 0 es el valor que debe salir de las tablas de aproximación.

Goldschmidt

El método de Goldschmidt para división y aplicada también para raíces cuadradas, surgió de la tesis de graduación de maestría de Ingeniería Eléctrica del MIT por parte de Robert Goldschmidt en 1964. Esta técnica se basa en la aproximación de la raíz cuadrada por medio de productos sucesivos donde si b_0 es el valor de la base de la raíz cuadrada se busca que se cumpla que $b_n = b_0 Y_0 Y_1 \dots Y_n = 1$.

El método de Goldschmidt es ideal para aplicaciones que implementan de forma separada la multiplicación de la suma y en general se emplea en multiplicadores en pipeline. Un detalle de este método es que

Las ecuaciones (2.4) y (2.5) son necesarias para el cumplimiento de este método numérico. El método de Goldschmidt, contrario al de Newton, no es autocorregible lo cual implica que existan errores acumulados.

$$b_i = b_{i-1} Y_{i-1}^2 \quad (2.4)$$

$$Y_i = (3 - b_i)/2 \quad (2.5)$$

2.6 Punto fijo sin signo

Una palabra de N-bits cuando es representada en la forma de un número racional en punto fijo, puede tomar los valores dados por el subconjunto P

pertenecientes a los racionales no negativos como se observa en la ecuación (2.6).

$$P = \{p/2^b \mid 0 \leq p \leq 2^N - 1, \quad p \in \mathbb{Z}\} \quad (2.6)$$

En la ecuación anterior se tiene que P contiene 2^N elementos. Además la nomenclatura P(a,b) representa el subconjunto P, suponiendo que $a = N - b$.

Por otra parte, el valor de un número binario de N-bits X, perteneciente al subconjunto P está dado por la ecuación (2.7).

$$X = (1/2^b) \sum_{n=0}^{N-1} 2^n x_n \quad (2.7)$$

donde X_n representa el bit n del número X. El rango de números que puede tomar como representación el número X es de 0 hasta $(2^N - 1)/2^b = 2^a - 2^{-b}$.

La representación binaria de un número X en punto fijo de 6-bits donde $b = 2$, tiene la forma de $x_3x_2x_1x_0x_{-1}x_{-2}$.

2.7 Verificación funcional

3 Desarrollo de la aplicación

3.1 Generalidades

En esta sección se presentan generalidades acerca de la implementación del algoritmo de generación de rayos y de las operaciones necesarias para generar los vectores en el dominio del espacio.

Vectores normalizados

Los vectores normalizados en el espacio están dados por un punto Y que se dirige a un punto X , por lo cual se sabe que $X-Y$ es la magnitud sin normalizar del vector, por lo que se necesita posteriormente dividir entre la raíz cuadrada del valor absoluto $X-Y$, para así lograr obtener el vector normalizado que requiere la Unidad de Generación de Rayos (RGU) a su salida.

$$F = \frac{X - Y}{\sqrt{|X - Y|}} \quad (3.1)$$

Por la ecuación (3.1) se puede apreciar que se necesita obtener el inverso de la raíz cuadrada de la resta de los dos puntos en el espacio para lo cual se necesitaría de la capacidad de calcular la raíz cuadrada de un vector, dado lo anterior lo que sigue es definir las operaciones mínimas para obtener el inverso de la raíz cuadrada dentro de un intervalo de valores.

Elección del Newton Raphson

Dentro de los métodos multiplicativos para realizar el cálculo del inverso de la raíz cuadrada se tenían dos métodos principales: el método de Newton-Raphson y el método de Goldschmidt.

De estos dos métodos empleados en la aproximación de divisiones se puede observar que el método de Goldschmidt a la hora de adaptarse para el cálculo de la raíz cuadrada adquiere casi la misma forma que el método de Newton-Raphson adaptado a las raíces cuadradas, además que el método de Goldschmidt está diseñado para calcular dos iteraciones (el numerador y el denominador) por lo que está más orientado a estructuras que usen de manera intensiva pipeline como la Unidades de Punto Flotante.

Por otra parte los métodos sustractivos como el método SRT implican el uso de muchas estructuras de hardware especializadas que se realizan varias

iteraciones de corrimientos para la correcta aproximación de un resultado por lo que además resulta ser un método lento en comparación con los métodos multiplicativos.

3.2 Operaciones con el método de Newton Raphson

El método de Newton-Raphson para la aproximación del inverso de la raíz cuadrada entonces se puede desglosar en dos partes:

1. Obtención de una aproximación de la raíz cuadrada
2. Iteración sobre la aproximación de la raíz cuadrada

Se necesita una aproximación muy precisa que facilite la convergencia rápida al valor del inverso de la raíz cuadrada por lo cual se guardan algunos valores en una memoria (LookUp Table) que permitan un valor inicial lo suficientemente robusto como evitar múltiples iteraciones innecesarias que implicarían varios ciclos de reloj.

Por medio de iteraciones sobre la aproximación obtenida de una tabla se puede mejorar tal valor del inverso de la raíz, empleando básicamente solo tres operaciones:

1. Resta
2. Multiplicación
3. Un corrimiento hacia la izquierda

Dado que la implementación del RGU se realiza en un FPGA que posee al interior módulos de multiplicación incrustados es innecesario diseñar un sistema de multiplicación convencional en la descripción en Verilog.

Con respecto al corrimiento hacia la izquierda esta operación corresponde al dos en el denominador que se halla en la ecuación (2.3).

3.3 Consideraciones del Punto Fijo

La multiplicación de números enteros no presenta mayor complicación, pero el inconveniente proviene cuando se intentan realizar operaciones en formato de punto fijo.

En el formato de punto fijo se define una cantidad de bits que representan la parte entera, y la restante cantidad de bits representan la parte fraccionaria del número (esta parte se corresponde a la escala).

Cada vez que se multiplica resulta que el número resultante se aumenta respecto a la cantidad de bits que tenga la parte fraccionaria, lo cual implica que se debe tener un registro para resultados lo suficientemente grande para no perder los bits que se puedan perder por tal efecto.

Después de haber realizado la multiplicación se puede desplazar los bits hacia la izquierda una cantidad de veces igual al número de la escala en cuestión con el fin de obtener un resultado del mismo tamaño de bits que los operandos.

Al final esto deriva en una operación de multiplicación especial con respecto a la que se suele usar.

La resta de números en punto fijo permanece intacta ya que se mantiene igual el número de bits del resultado de tal operación.

3.4 Estructura del RGU

La Unidad de Generación de Rayos (RGU) usa dos instancias de memorias: una para las instrucciones y otra para el almacenamiento de datos. La tarjeta Papilio que ha implementado el modelo del GPU Theia posee una memoria DRAM lo cual facilitaría enormemente el acceso a memoria y permitiría al dispositivo tener una mayor programabilidad.

Por lo anterior se puede apreciar que el RGU tiene la capacidad de programar las instrucciones básicas que tiene así como su orden, con el objetivo de permitir la experimentación del dispositivo así como explotar las capacidades de debugging que posee las instrucciones del GPU Theia por medio de la comunicación serial que tiene gracias debido a un IP de Xilinx.

La RGU también tiene una instrucción especial llamada PUSH que habilita a la cola que hay a la salida del RGU almacenar el valor que se calculó por medio de la tabla (LUT) y las iteraciones.

Por otra parte por el momento las instrucciones del RGU deben ir intercaladas por instrucciones NOP ya que existen "data hazards"(peligros de datos) debido a que no se ha planteado el uso de pipeline en los datos, pero es de fácil implementación, y estará implementado en la versión final del proyecto.

3.5 Instrucciones de iteración

A continuación se plantean las instrucciones necesarias (en pseudocódigo) para la ejecución del método de Newton-Raphson para el cálculo de la raíz cuadrada.

Algorithm 2 Método de Newton-Raphson

```
1: procedure NEWTON-RAPHSON PARA RN
2:   Busque en  $X$  en LUT para hallar  $R0$ 
3:   for do cada iteración  $i$  hasta  $N$ 
4:     Multiplique  $Ri$  por  $Ri$  y guarde en  $S0$ 
5:     Multiplique  $X$  por  $S0$  y guarde en  $S1$ 
6:     Reste  $X$  menos  $S1$  y guarde en  $S2$ 
7:     Multiplique  $S2$  por  $Ri$ 
8:     Desplace un bit a la izquierda a  $S2$  y guarde en  $Ri$ 
9:   Enviar dato válido
```

4 Resultados

