revista moondak

disponible cada domingo

El aprovhechamiento de las FPGA para la aceleración de la

Cryptografía

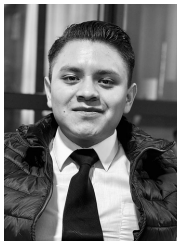
Para dummies

La ciencia que protege la nueva era digital

Curiosidades, misterios, conceptos, ... Lo más interesante.

MOONDAK

La revista científica con los temas más interesantes



Las FPGA, criptografía y criptomonedas

JOSÉ DANIEL RUPERTO VILLALPANDO

Estudiante de ingeniería informática | TESCHA

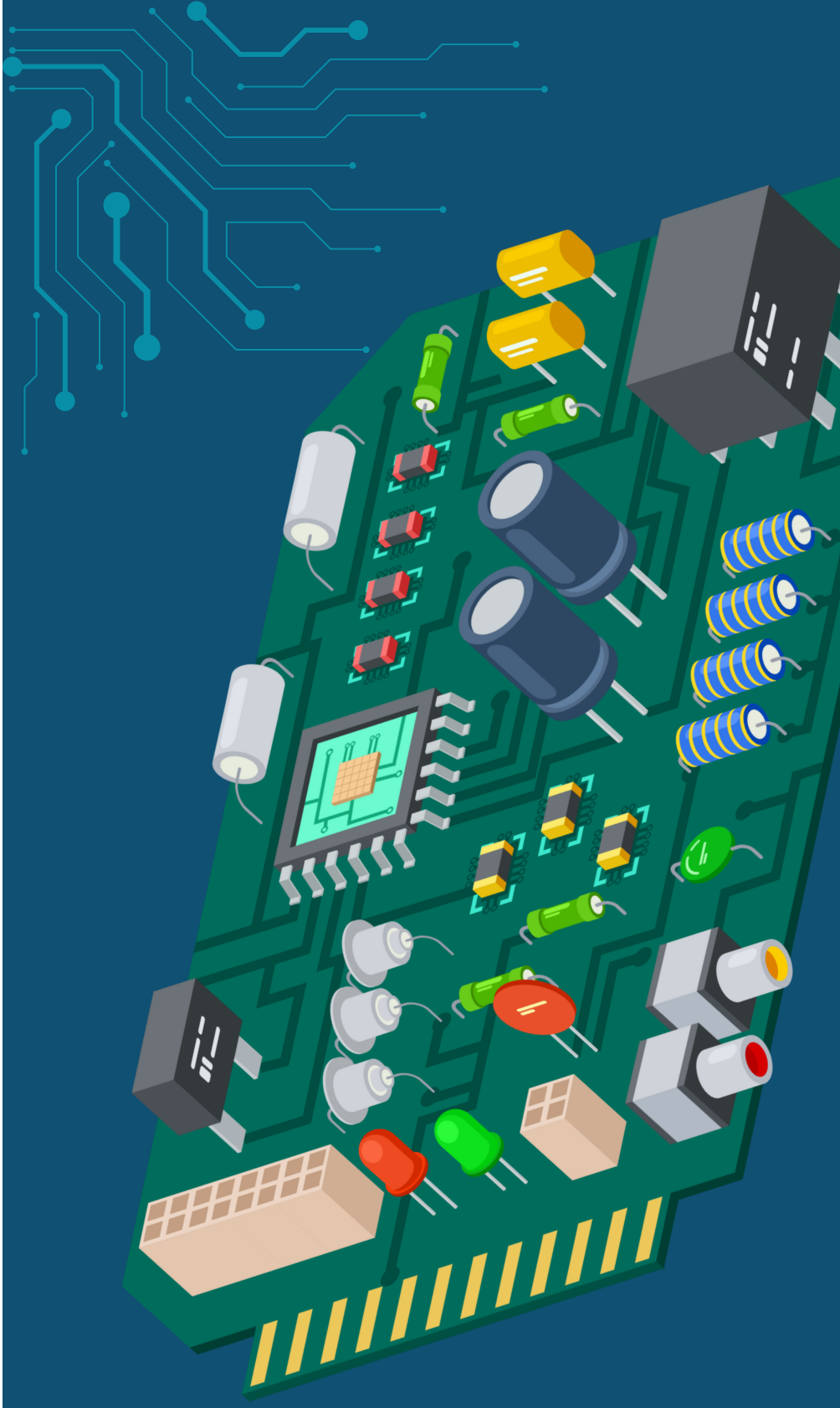
¿QUÉ SON LAS FPGA?

¿Qué los caracteriza?

Las FPGA son las siglas de Field Programmable Gate Array, o en español Matriz de Puertas Programables en Campo. Estos son unos diminutos dispositivos semiconductores que tienen la capacidad de programarse para realizarse acciones muy concretas de forma rápida y eficiente,.

A pesar de que existen desde hace algún tiempo, no son dispositivos muy usuales. Sin embargo, los FPGA cuentan con una característica que los hacen únicos en distintas aplicaciones. Los FPGA tienen la capacidad que pueden reprogramarse.

Inicialmente los FPGA se caracterizaban por ser lentos, consumir grandes cantidades de energía y tener poca capacidad de cómputo paralelo. Sin embargo, esto ha cambiado gracias a las mejoras introducidas a la tecnología del silicio y al desarrollo de sistemas programables. Esto se ha traducido en una mejora sustancial en términos de velocidad y capacidad de trabajo en paralelo. Transformando a los FPGA en candidatos perfectos para aplicaciones de alta demanda de poder cómputo.



Los circuitos integrados (CI) generalmente se llaman "chips". Implementan circuitos electrónicos muy pequeños sobre un sustrato de silicio. Las CPU, las GPU y FPGAs son todos circuitos integrados. La mayoría de los CI implementan el diseño lógico. Las señales eléctricas entran en un CI y se interpretan como un "0" o como un "1" en función de su nivel de voltaje. Puedes mirar diferentes señales para reunir muchos valores, o puedes mirar la misma señal muchas veces diferentes y ver cómo cambia.

CRIPTOGRAFÍA

Acerca de la criptografía

La criptografía es el proceso de ocultar o codificar información para que solo la persona a la que se destinó un mensaje pueda leerlo. El arte de la criptografía se ha utilizado para codificar mensajes durante miles de años y continúa utilizándose en tarjetas bancarias, contraseñas de computadoras y comercio electrónico

TIPOS DE CRIPTOGRAFIA

criptografía de clave simétrica

El cifrado simétrico requiere que todos los destinatarios del mensaje tengan acceso a una clave compartida.

criptografía de clave asimétrica

Estos se basan en problemas matemáticos que son relativamente fáciles de hacer en una dirección, pero que no se pueden invertir fácilmente.

HASH EN CRIPTOGRAFÍA

Una función hash criptográfica es una herramienta para convertir datos arbitrarios en una “huella digital” de longitud fija. Las funciones hash están diseñadas para que sea difícil encontrar dos entradas diferentes que tengan la misma huella digital, y es difícil encontrar un mensaje cuya huella digital coincida con un valor fijo.

FIRMA DIGITAL

Los esquemas de firma digital son un tipo de criptografía de clave pública que garantiza la integridad, autenticidad y no repudio de los datos. Esta firma es única para el par documento/clave privada, y puede adjuntarse al documento y verificarse con la clave pública de la persona que firma.

CIFRADO HÍBRIDO

El cifrado híbrido se utiliza de manera generalizada en los protocolos de transferencia de datos para la web, como en la seguridad de la capa de transporte (TLS). Cuando se conecta a un sitio web que utiliza HTTPS (HTTP seguro con TLS), el navegador negociará los algoritmos criptográficos que aseguran la conexión. Estos incluyen algoritmos para el intercambio de claves, cifrado simétrico y firmas digitales.

MONEDAS CRIPTOGRÁFICAS

Acerca de las criptomonedas

Una criptomoneda es una moneda digital, que es una forma alternativa de pago creada utilizando algoritmos de cifrado. El uso de tecnologías de cifrado significa que las criptomonedas funcionan tanto como moneda como sistema de contabilidad virtual.
Para usar criptomonedas, necesita una billetera de criptomonedas. Estas billeteras pueden ser software que es un servicio basado en la nube o que se almacenen en su computadora o en su dispositivo móvil. Las billeteras son la herramienta a través de la cual almacena sus claves de cifrado que confirman su identidad y se vinculan a su criptomoneda.

Funcionamiento

Los bitcoins operan en Internet, pueden ser transferidos directamente de persona a persona, y se almacenan en monederos electrónicos que se descargan en el computador o en el teléfono móvil. Permiten acceder a una dirección que contiene una llave privada y una irma criptográica para demostrar la propiedad del usuario. Las transacciones se conirman mediante un proceso minucioso llamado minería. Cuando existen varias transacciones, veriicadas de manera criptográica por los miembros de la red, se empaquetan en un bloque que ingresa a la cadena de bloques o blockchain por donde pasan todas las operaciones de bitcoins.

Minado

En las redes de criptomonedas, el minado es una validación de las transacciones. Por este esfuerzo, los mineros obtienen unidades como recompensa. Esta recompensa disminuye las tarifas, creando un incentivo complementario para contribuir al poder de procesamiento de la red. El ratio de generación de nuevos hashes que validan transacciones ha aumentado gracias al uso de máquinas especializadas como FPGAs y ASICs

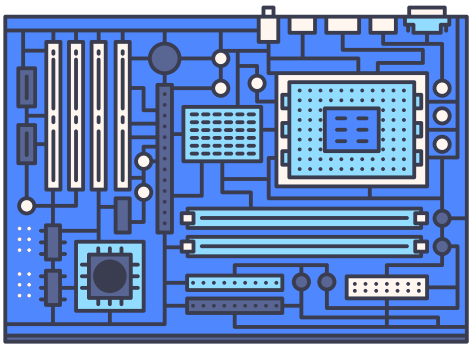
USO DE LAS FPGA PARA LA ACELERACIÓN DE

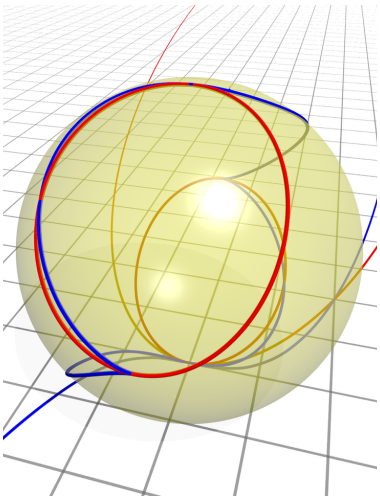
CRIPTOGRAFÍA

ACELERACIÓN POR FPGA

El concepto general tras la utilización de esta tecnología, es que un algoritmo complejo computacionalmente demandante, se mueva de una aplicación ejecutándose sobre el CPU a un acelerador implementado sobre la FPGA. Cuando la aplicación requiere una tarea acelerada, el CPU transmite los datos y sigue con sus tareas, la FPGA los procesa y los retorna para su posterior utilización, liberando al CPU de dicha tarea y ejecutándola en menor tiempo.

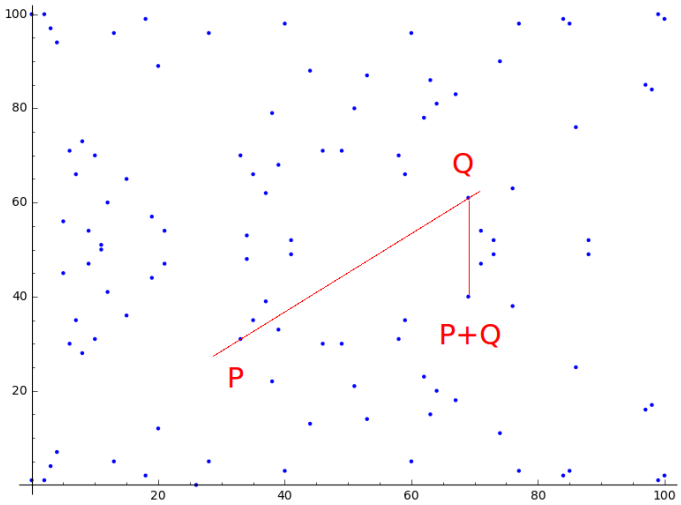
El factor de aceleración a obtener, dependerá del algoritmo, la cantidad y tipo de datos. Puede esperarse desde unas pocas veces hasta miles, que en procesos que llevan días de computo se traduce bajarlo a horas o minutos. Esto no solo es una mejora en la experiencia de usuario, sino que también una disminución del costo energético y de infraestructura.





CRIPTOGRAFÍA DE CURVAS ELÍPTICAS

Una de las mejores técnicas en criptografía es el denominado criptosistema de curvas elípticas (conocido formalmente como ECC, por sus siglas en inglés). La investigación actual en ECC se centra en mejorar los métodos aritméticos necesarios para operar sobre las curvas elípticas. Esto implica el cálculo de los puntos sobre las curvas en un campo finito que sir ven para propósitos criptográficos.



MULTIPLICACIÓN DE PUNTOS

La fundamental y más costosa operación en el criptosistema de curvas elípticas es la multiplicación de puntos o multiplicación escalar kP, donde k es un entero y P es un punto de la curva elíptica. La multiplicación escalar se define en términos de la suma:

$$kP = \underbrace{P + P + \ldots + P}_{\text{k veces}}$$

En algunas aplicaciones es conveniente representar los puntos racionales en coordenadas proyectivas, lo cual provee una disminución en el número de inversiones re-queridas, lo que se traduce en mayor facilidad de implementación.

TECNOLOGÍAS HARDWARE

En general, las FPGA's no son dispositivos finales para el diseño, por el contrario, es una plataforma de pruebas donde el circuito es evaluado y depurado. De esta manera, cuando el diseño está listo para su producción en masa, es implementado en los llamados VLSI o "Very Large Scale Integration" , que son circuitos integrados de función específica, los cuales son más baratos y rápidos que una FPGA pero mucho menos flexibles.

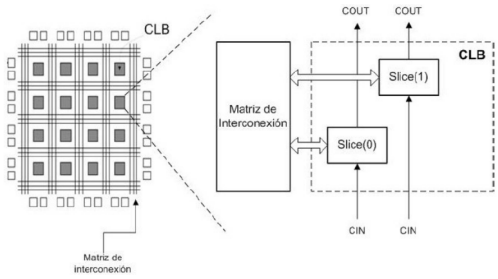
ESTRUCTURA

La compañía Xilinx divide sus 14 modelos de FPGA en distintas familias con base en su tamaño y características, de esta manera dependiendo del presupuesto y los requerimientos, se elige la familia de FPGA adecuada a las necesidades del proyecto

Hay distintas familias como las Spartan (de uso prácticamente académico), Kintex, Artix(de uso principalmente industrial) y Virtex. Otras empresas vendedoras y fabricantes de FPGA's son Atmel, Altera, AMD o Motorola.

Dentro de las FPGA's se encuentra una estructura jerarquizada de componentes unos dentro de otros. En esta jerarquía se encuentran en primer lugar los bloques configurables CLB's o en ingles "Configurable Logic Blocks" los cuales están conectados directamente a una matriz de interconexión donde se realizan las conexiones reconfigurables. Dentro de estos CLB's podemos encontrar varias unidades de componentes llamados "Slices"(Figura 1). Los "Slices" están formados por multiplexores y elementos reconfigurables llamados LUT's o "Look Up Tables" que pueden usarse como bloque de memoria o un elemento de lógica. El número de "Slices" requeridos en una implementación es considerado una métrica para definir el tamaño del diseño.

Se ha terminado concluyendo en vista de las características vistas de todas las familias que la familia de uso sea la Virtex5 debido a sus características con respecto a la velocidad y otros recursos que pueden ser utilizados en futuras mejoras para el componente final del trabajo. Además la familia Virtex5 ofrece una gran cantidad de componentes llamados "DSP48Slices" que son elementos para procesamiento digital de señales, los cuales son capaces de realizar multiplicaciones asimétricas de 25x18 bits y sumas de 48 bits.



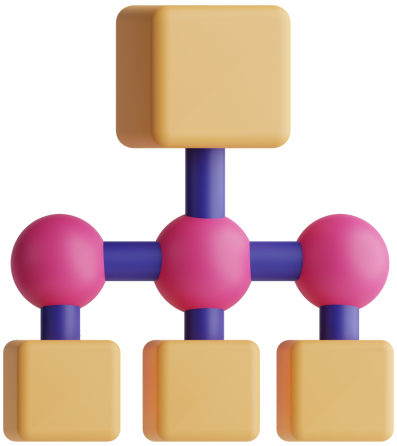
REDUCTORES Y ALGORITMOS

REDUCTORES

Dentro de las diferentes versiones y algoritmos de un reductor modular se han escogido 3 candidatos para hacer un estudio de las diferentes funcionalidades y características orientadas objetivo final de incremento de velocidad. Los 3 algoritmos de reducción candidatos son: El algoritmo naive a base de restas, el algoritmo de Barret y el algoritmo de Montgomery.

La reducción de Barret es el método que puede calcular un módulo de una forma más rápida que el método tradicional a base de restas y fue introducido por P.D.Barrett en [15]. La reducción de Barret requiere de un dato adicional denominado constante μ. Esta constante se obtiene haciendo una división entera entre el módulo y un valor que depende de k (el ancho del valor del módulo).

La reducción de Montgomery tiene la característica básica de permitir el cálculo eficiente de multiplicaciones modulares sin necesidad de hacer divisiones. El no necesitar divisiones enteras es de gran interés para reducir el coste computacional de los algoritmos de cálculo de reducciones modulares con números grandes.



ALGORITMOS

Cada uno de los reductores afronta la operación de diversas formas. Mientras unos se basan en una constante además de multiplicaciones, otros cambian de representación. A continuación se pueden ver las diferentes formas de calcularlo para cada reductor.

Algoritmo naive

El método naive para el cálculo del módulo de un número se basa principalmente en la idea primitiva de la división. El algoritmo resta sucesivas veces el valor del módulo a un resultado parcial, que toma el valor de la entrada al principio, hasta que tiene un valor inferior al del módulo.

Algoritmo de Barret

El algoritmo de reducción de Barret se basa principalmente en la pre-computación de una constante μ que conociendo la entrada del módulo puede ser guardado en un registro o bien, mediante señales fijas.

Algoritmo de Montgomery

El algoritmo de Montgomery es un algoritmo que antes de poderse ejecutar necesita de ciertas verificaciones. Para que funcione correctamente se necesita que teniendo m, R y A, donde A es la entrada, m el módulo y R valor auxiliar. $0 \leq A \leq m \cdot R$

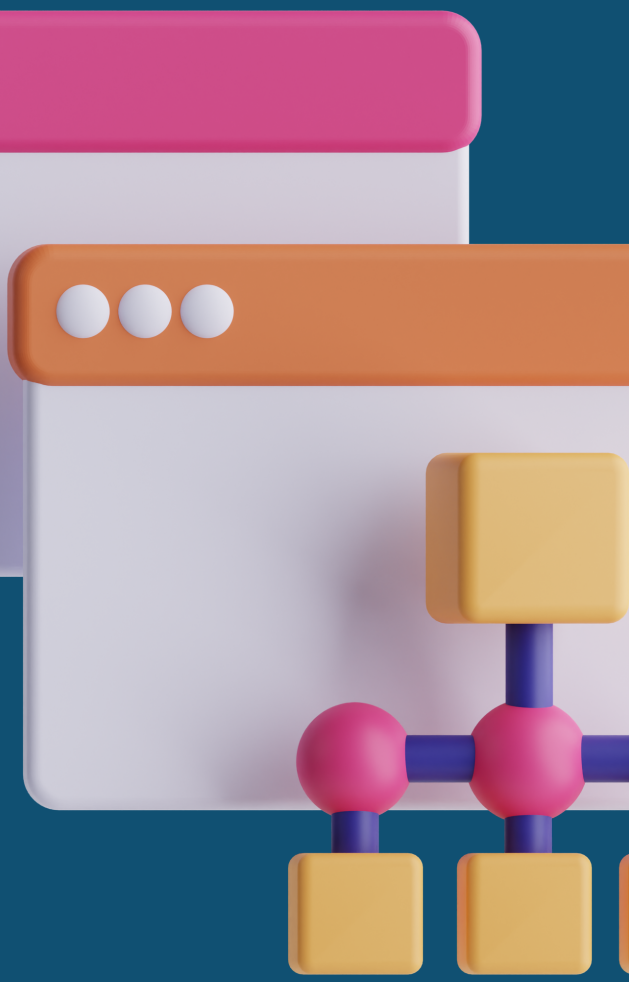
Algoritmo de Karatsuba-Offman

El algoritmo de Karatusuba-Ofman se basa principalmente en la división de los elementos de la multiplicación en 2 partes más pequeñas y de igual dimensión. En este algoritmo, para entradas de n bits, se realizan cuatro multiplicaciones de n/2 dígitos, 2 operaciones de desplazamiento a izquierda, 1 suma de n dígitos y dos sumas de 2n dígitos.

Algoritmo de Booth

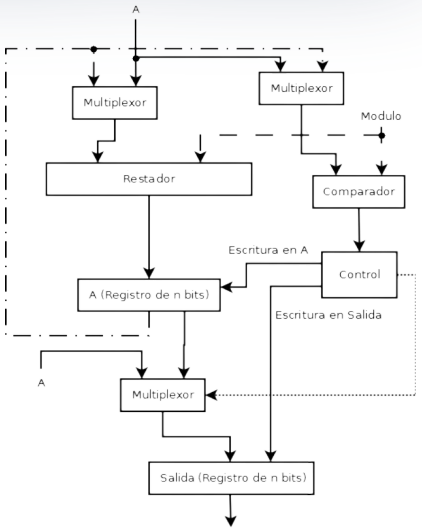
El algoritmo de Booth examina los pares adyacentes de los bits menos significativos del multiplicador. Se añade un bit extra que se coloca en la posición menos significativa del bit menos significativo del multiplicador.

ARQUITECTURA DE ALGORITMOS

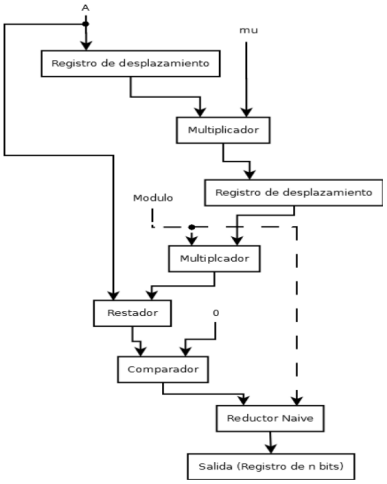


El reductor naive

Es el reductor más simple que se conoce. Gracias a que tiene muy pocos componentes, (2 registros, el módulo de control, el restador, el comparador y varios multiplexores). Este reductor ocupa muy poco área. El módulo de control es fácilmente implementable con una máquina de estados o un contador de modo que en cada estado se activan las señales de control correspondientes. Este reductor actúa en base al resultado del comparador.



Rico P, Aceleracion hardware con propósitos criptográficos, p.52.

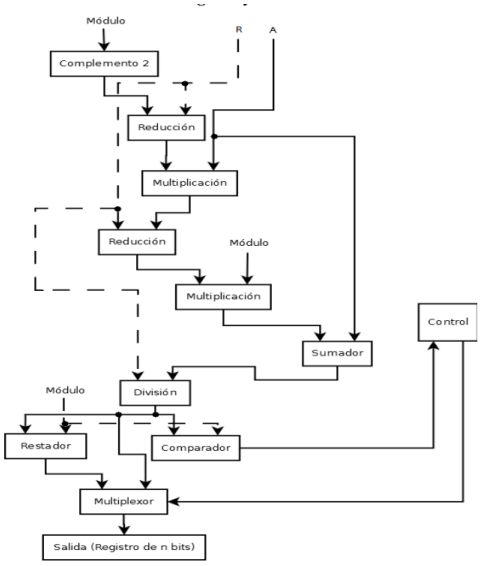


Rico P, Aceleracion hardware con propósitos criptográficos, p.53.

Algoritmo de Barret

El módulo de control es fácilmente implementable con una máquina de estados o un contador de modo que en cada estado se activan las señales de control correspondientes. Dado que el último paso del algoritmo es un bucle “while” similar al reductor naive, se ha utilizado el módulo de reducción naive para ese paso del algoritmo.

El multiplicador reductor de Montgomery es el reductor más complejo. No sólo por que tenga la multiplicación sino por el propio algoritmo. Como se mencionó antes si R está en base 2 las divisiones y reducciones se pasan a ser triviales. En este caso R está dentro del sistema y se ejecutan las operaciones en base a ese R especificado en el diseño. Es interesante ver como calcula el módulo aunque para ello necesite más valores que los demás reductores

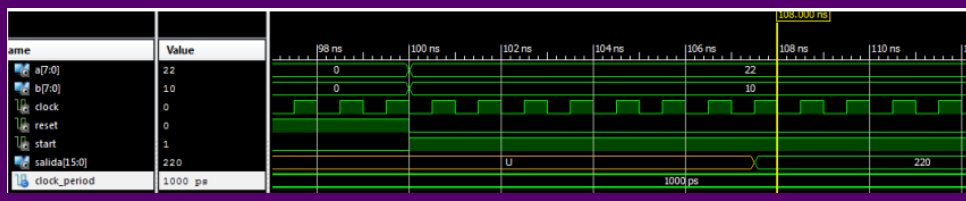


Rico P, Aceleracion hardware con propósitos criptográficos, p.55.

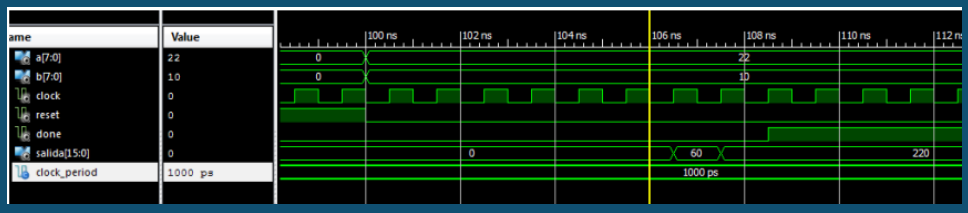
RESULTADOS TEÓRICOS

ALGORITMO DE SUMAS Y DESPLAZAMIENTOS

La simulación del primer multiplicador muestra como una multiplicación de 8 bits tarda 8 ciclos de reloj. Estos corresponden al número de bits de ancho de las entradas.. La frecuencia del reloj en esta simulación no corresponde a la frecuencia que soporta el componente sino que se ha reducido para poder mostrarlo.



Rico P, Aceleracion hardware con propósitos criptográficos, p.72.



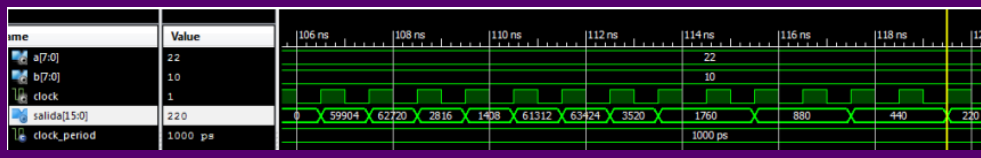
Rico P, Aceleracion hardware con propósitos criptográficos, p.73.

ALGORITMO DE KARATSUBA-OFMAN

La simulación del multiplicador de Karatsuba-Ofman muestra como una multiplicación de 8 bits que tarda 9 ciclos de reloj. Siguiendo la formula (4*1)+5 que corresponde al número de ciclos del caso base más 4 por el número de niveles que tiene que hacer la recursión (1 en este caso ya que el caso base es 2x2 bits)

ALGORITMO DE BOOTH

La simulación del multiplicador de Booth muestra como multiplicación de 8 bits que tarda 12 ciclos de reloj. Estos corresponden a la ecuación vista 2+x+2y y el número 22 en binario (00010110). La ecuación con los datos quedaría de la siguiente forma: 2+4+2*3. La frecuencia del reloj en esta simulación no corresponde a la frecuencia que soporta el componente sino que se ha reducido para poder mostrarlo.



Rico P, Aceleracion hardware con propósitos criptográficos, p.73.

La reducción de Barret ofrece un número bastante bueno con respecto a los demás módulos. En una comparación justa, con Barret calculando la constante μ y con Montgomery sin optimizar para ningún módulo Barret obtiene una velocidad con anchos de banda bajos (entre 0 y 1024 bits) bastante buena frente a otros algoritmos como el de Montgomery que permanecen casi constantes

Reducción	k	LUT's	Flip-Flop's	Periodo	Ciclos	Tiempo total
Naive	32	724	117	4.266 ns	*A/m*	*A/m · Periodo*
	64	1695	208	5.133ns	*A/m*	*A/m · Periodo*
	128	3616	424	6.036ns	*A/m*	*A/m · Periodo*
Barret	32	7844	23897	4.611 ns	56	258.216 ns
(Sin cálculo μ)	64	30229	8169	5.083 ns	60	304.980 ns
(Con cálculoμ)	32	8820	2228	4.697ns	571	2681.987 ns
Montgomery	32	293	107	1.397ns	52	72.644 ns
	64	634	271	1.971ns	100	197.100 ns
	128	1277	529	2.835ns	196	555.66 ns

AUTORES

JOSÉ DANIEL RUPERTO VILLALPANDO

DULCE ARISBETH CORDOBA BELTRÁN

Estudiantes de ingeniería informática | TESCHA

CONTACTO

JOSÉ DANIEL RUPERTO VILLALPANDO

FUENTES CONSULTADAS

Rico, J. P. (2013, septiembre). Aceleración hardware con fines criptográficos. Recuperado el 7 de abril de 2024, de Ucm.es website: https://docta.ucm.es/entities/publication/32cd993b-0fe5-41b3-a1ee-6f185e735a48

Bit2me, ¿Qué son las FPGA?, Recuperado el 6 de abril de 2024, de https://academy.bit2me.com/que-es-fpga/

What is cryptography? (s/f). Fortinet. Recuperado el 6 de abril de 2024, de https://www.fortinet.com/lat/resources/cyberglossary/what-is-cryptography

What is cryptographic, Amazon.com. Recuperado el 7 de abril de 2024, de https://aws.amazon.com/es/what-is/cryptography/

Centro de Investigación de la Universidad Distrital Francisco José de Caldas. (s/f). Recuperado el 7 de abril del 2024 de https://revistas.udistrital.edu.co/index.php/visele/article/view/3515/5076


MOONDAK