Parte 2 del proyecto: RTL, síntesis, placement y STA

Isaac F. Fonseca Segura
Escuela de Ingeniería Eléctrica
Universidad de Costa Rica
San José, Costa Rica
Email: isaac.fonsecasegura@ucr.ac.cr

***Resumen*—En este proyecto se implementa el módulo para minar hashes planteado en la primera parte mediante un modelo de alto nivel. Se proponen dos versiones, una para optimizar el rendimiento y otra para optimizar el área.**

INTRODUCCIÓN

Partiendo del modelo de alto nivel implementado en la primera parte del proyecto se implementaron a nivel del RTL los mismos módulos que se habían propuesto, con una ligera alteración al módulo de cálculo de hash para la versión de rendimiento.

Una vez con las las implementaciones en RTL se realizó la síntesis con Yosys [1] mediante la heramienta Qflow [2]. Con esta misma se realizó el placemente y el STA.

14 de junio, 2021

I. RESULTADOS

En esta sección se muestran los resultados obtenidos de ambas propuestas de diseño. En los datos a continuación se muestra el resultado del primer bounty encontrado con el modelo de alto nivel. Se observa que el resultado para un target 0A es 040939.

```
Se ha encontrado un bounty!
Input:  [0x39, 0x7d, 0x9f, 0x2f, 0x40,
0xca, 0x9e, 0x6c, 0x6b, 0x1f, 0x33, 0x24,
0x0, 0x0, 0x35, 0xf]
Target:  0xa
Hash:  [0x4, 0x9, 0x39]
Número de iteraciones:  13584
Tiempo de ejecución: 76.293945
microsegundos
```

I-A. Diseño optimizado en área

En la Figura 1 se observa como además del primer bounty se encuentran otros. Es importante observar en la Figura 2 que el primer bounty corresponde al mismo encontrado por el módulo de alto nivel,y que le toma 13584 iteraciones encontrar este primer bounty, igual que en modelo de alto nivel.

Respecto a los datos encontrados en los *logs*, estos se muestran a continuación. Se muestra la cantidad total celdas, 4566, de las cuales 4534 son combinacionales y 32 secuenciales. Entre las combinacionales hay 125 buffers y 778 inversores. Además hay 4215 cables.

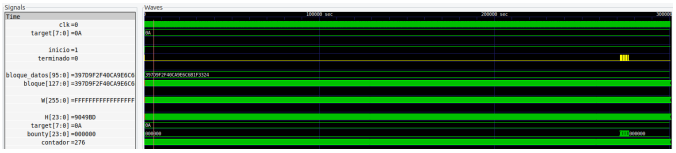

Figura 1. Resultados del diseño optimizado en área.

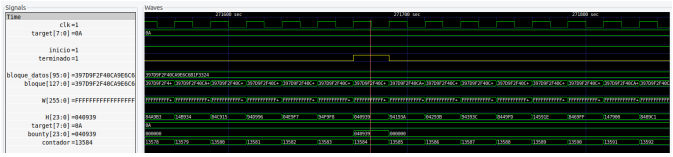

Figura 2. Primer bounty encontrado con diseño optimizado en área.

En el archivo DEF generado por la herramienta de layout de Qflow [2] se indica que las unidades de longitud están basadas en 100 µm, por lo que el die tiene un área de 0.2522 mm^2, con una densidad de placement de 0.6.

La frecuencia máxima que puede alcanzar el circuito según la herramienta de STA es de 69.7708 MHz. Con dicha frecuencia el **tiempo de cálculo** para obtener un bounty que requiere iterar el nonce 1000 veces es de 14.3326 µs.

```
=== micro_ucr_hash ===
   Number of wires:                4215
   Number of cells:                4566
     AND2X2                         105
     AOI21X1                        577
     AOI22X1                         10
     BUFX2                          125
     DFFPOSX1                        32
     INVX1                          778
     NAND2X1                        542
     NAND3X1                        963
     NOR2X1                         305
     NOR3X1                         133
     OAI21X1                        704
     OAI22X1                          9
     OR2X2                           95
     XNOR2X1                        132
```

```
    XOR2X1                          56

----------------------------
UNITS DISTANCE MICRONS 100 ;
DIEAREA ( -320 -300 ) ( 58880 42300 ) ;
----------------------------
Computed maximum clock frequency (zero
margin) = 69.7708 MHz
----------------------------
```

I-B. Diseño optimizado en desempeño

En la Figura 3 se muestra el módulo de rendimiento trabajando de manera correcta, se pueden observar los cuatros submódulos internos calculando hashes de forma paralela. Además en la Figura 4 se observa como el primer bounty que se encuentra corresponde al mismo encontrado por el modelo de alto nivel y por el diseño optimizado en área, lo que confirma el correcto funcionamiento, pero aún más importante es observar que el bounty se encontró con sólo 3395 iteraciones, contrario a 13584. Lo que teóricamente aumenta el rendimiento 4 veces, esto es correspondiente a que se usaron *4 módulos en pararelo*. Además este diseño termina después de realizar alrededor de mil millones de iteraciones, contrario al modelo de área que termina después de cuatro mil millones de iteraciones.

Figura 3. Resultados del diseño optimizado en rendimiento.

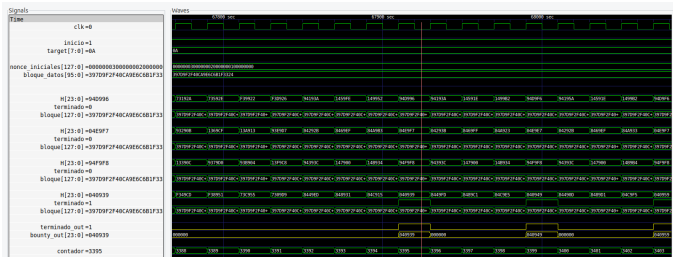

Figura 4. Primer bounty encontradoparalelización con diseño optimizado en rendimiento.

De nuevo, respecto a los datos del circuito, hay 18384 celdas, de las cuales 18256 son combinacionales y 128 secuenciales. Entre las combinacionales hay 25 buffers y 3160 inversores. Además hay 17412 cables. El área total del circuito es de 1.004 mm^2, con una densidad de placement de 0.6.

La frecuencia máxima que puede alcanzar el circuito según la herramienta de STA es de 67.8356 MHz, lo cual es muy similar al resultado obtenido para el diseño optimizado en área. Una explicación para que sea menor, es que el diseño optimizado en desempeño usa un módulo de control al final, lo cual hace el camino total un poco más largo. Con dicha frecuencia el **tiempo de cálculo** para obtener un bounty que requiere iterar el nonce 1000 veces es de 3.6853 µs, esto debido a la paralelización. Es decir, el módulo optimizado en rendimiento es 3.8891 veces más rápido que el módulo optimizado en área.

```
=== micro_ucr_hash_mod ===

   Number of wires:                 17412
   Number of cells:                 18384
     AND2X2                           404
     AOI21X1                         2480
     AOI22X1                           48
     BUFX2                             25
     DFFPOSX1                         128
     INVX1                           3160
     MUX2X1                             8
     NAND2X1                         2329
     NAND3X1                         3940
     NOR2X1                          1402
     NOR3X1                           532
     OAI21X1                         2788
     OAI22X1                           44
     OR2X2                            436
     XNOR2X1                          480
     XOR2X1                           180
----------------------------
UNITS DISTANCE MICRONS 100 ;
DIEAREA ( -320 -300 ) ( 118320 84300 ) ;
----------------------------
Computed maximum clock frequency (zero
margin) = 67.8356 MHz
----------------------------
```

II. Conclusión

Los dos diseños funcionan de manera correcta, y efectivamente el módulo optimizado en rendimiento mejora muchísimo en rendimiento, 3.8891 veces, pero aumenta el área unas 3.9810 veces respecto al diseño optimizado en desempeño.

Referencias

[1] YosysHQ, *YosysHQ/yosys*. dirección: https://github.com/YosysHQ/yosys.

[2] T. Edwards, *Qflow*. dirección: https : / / github . com / RTimothyEdwards/qflow.