รายงานวิชา 2100301

การฝึกงานวิศวกรรม (ENGINEERING PRACTICE)

จัดทำโดย นายนรวิศว์ หนังสือ

รหัสประจำตัว 5730289021

ภาควิชาวิศวกรรมไฟฟ้า คณะวิศวกรรมศาสตร์

จุฬาลงกรณ์มหาวิทยาลัย

หน่วยงานที่ฝึกงาน บริษัท ซิลิคอน คราฟท์ เทคโนโลยี จำกัด

เลขที่ 40 ถนนเทศบาลรังสรรค์เหนือ

ซอย 15 แขวงลาดยาว เขตจตุจักร

กรุงเทพฯ 10900

วิศวกรผู้ดูแล นายกานต์ โอภาสจำรัสกิจ

Member of Technical Staff

ช่วงระยะเวลาการฝึกงาน ตั้งแต่วันที่ 29 พฤษภาคม 2560

ถึงวันที่ 28 กรกฎาคม 2560

รวมระยะเวลาการฝึกงาน 9 สัปดาห์ / 42 วันทำการ / 305 ชั่วโมง

ศูนย์บริการจัดหางาน

ฝ่ายกิจการนิสิต

คณะวิศวกรรมศาสตร์

จุฬาลงกรณ์มหาวิทยาลัย

คำนำ

รายงานฉบับนี้เป็นจะแสดงให้เห็นถึงรายละเอียดของการฝึกงาน ตั้งแต่วันที่ ๒๙ พฤษภาคม ๒๕๖๐ ถึงวันที่ ๒๗ กรกฎาคม ๒๕๖๐ นับเป็นจำนวนวันทั้งหมด วันและคิดเป็นจำนวนทั้งหมด ชั่วโมง ณ บริษัท ซิลิคอน คราฟท์ เทคโนโลยี จำกัด ซึ่งเป็นการจำลอง(Simulation) และการสังเคราะห์(Synthesis) วงจรตามโจทย์ที่ได้รับมอบหมายจากทางบริษัทฯ

โครงสร้างของรายงานฉบับนี้แบ่งออกเป็น ๓ บท

บทที่ ๑ บทนำ

จะบอกวัตถุประสงค์ของการฝึกงาน ช่วงเวลาในการฝึกงานสภาพการทำงาน และผู้คุม

บทที่ ๒ รายละเอียดของหน่วยงาน

จะบอกถึงสถานที่ตั้ง ประวัติโดยย่อ และขอบเขตงานของบริษัท

บทที่ ๓ รายละเอียดของงานที่ทำ

จะบอกถึงเนื้องานที่ได้ทำ แนวคิดที่มี และผลลัพธ์ที่ได้ของโครงงานที่ได้ทำ และจะแบ่งออกเป็น 2 Part คือ Analog และ Digital

รายงานฉบับนี้ได้ถูกคาดหวังไว้ว่าจะมีประโยชน์แก่ผู้อ่านทุกท่านไม่มากก็น้อย และหากผิดพลาดประการใดก็ขออภัย ณ ที่นี้ด้วย

ผู้จัดทำ

นรวิศว์ หนังสือ

สารบัญ

บทที่ ๑ บทนำ

วัตถุประสงค์ของการฝึกงาน

เพื่อให้ผู้เรียนได้เพิ่มทักษะสร้างเสริมประสบการณ์ และพัฒนาวิชาชีพตามสภาพความเป็นจริงในสถานประกอบการ และเป็นแนวทางในสถานการณ์ประกอบอาชีพ ซึ่งจะทำให้รู้ถึงสภาพปัญหา และวิธีการแก้ไขปัญหาที่เกิดขึ้นอย่างมีเหตุผล สร้างความรับผิดชอบ มีระเบียบวินัย และการทำงานร่วมกับผู้อื่นอย่างมีประสิทธิภาพ รวมทั้งทำให้มีเจตคติที่ดีในการทำงาน มีความภูมิใจในวิชาชีพ และสุดท้ายเพื่อให้เป็นไปตามหลักเกณฑ์ของการสำเร็จการศึกษาตามหลักสูตรที่คณะวิศวกรรมศาสตร์ได้กำหนด

ช่วงเวลาในการฝึกงาน

๙.๐๐ น. ถึง ๑๘.๐๐ น. ช่วงพัก ๑๒.๐๐ น. ถึง ๑๓.๐๐ น.

สภาพการทำงานในระหว่างฝึกงาน

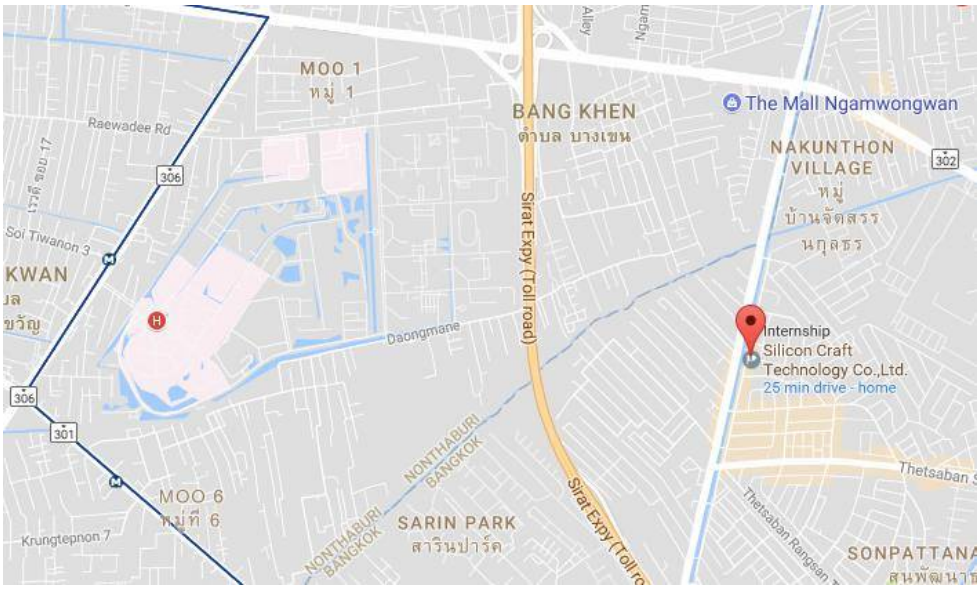
สถานที่ฝึกงานนั้นอยู่ในห้องประชุม อันเนื่องมาจากว่าทางบริษัทฯยังไม่พร้อมในเรื่องของพื้นที่(ชั้น ๕) ดังนั้นผู้ฝึกงานจึงได้ทำงานร่วมกับผู้ฝึกงานท่านอื่นๆในห้องประชุมเป็นส่วนใหญ่ ซึ่งทำให้ได้บรรยากาศที่ค่อนข้างอบอุ่นและไม่กดดัน

ผู้คุมการฝึกงาน

ผู้คุมนั้นเป็นจะค่อนข้างให้เสรีภาพในการทำงานเป็นส่วนใหญ่ เนื่องจากว่าการฝึกงานนั้นเป็นการให้โจทย์และให้ทางผู้ฝึกงานหาวิธีทำและจำลองวงจรจนได้ผลลัพธ์ออกมา ดังนั้นการฝึกงานแบบนี้จะค่อนข้างเข้ากับบุคลิกของคนส่วนใหญ่เป็นอย่างมาก

บทที่ ๒ รายละเอียดของหน่วยงาน

ที่ตั้ง



เลขที่ ๔๐ ถนนเทศบาลรังสรรค์เหนือ ซอย ๑๕ แขวงลาดยาว เขตจตุจักร

กรุงเทพมหานคร ๑๐๙๐๐

ประวัติโดยย่อ

บริษัทซิลิคอน คราฟท์ เทคโนโลยี ก่อตั้งขึ้นในปีพ.ศ. 2545 โดยได้นำเสนอผลิตภัณฑ์วงจรรวมเฉพาะงาน (ASIC) สำหรับการระบุค่าประจำตัวด้วยคลื่นวิทยุ (RFID) ที่มีฟังก์ชันการทำงาน และสมรรถนะสูงสอดคล้อง กับความต้องการของลูกค้า จุดแข็งในการออกแบบผลิตภัณฑ์ของบริษัทฯ อยู่ที่ความสามารถในการออกแบบวงจรรวมประเภทแอนะล็อก และสัญญาณผสมซึ่งผลงานได้รับการพิสูจน์แล้วในระดับโลก ซึ่งบริษัทฯ เป็นผู้ออกแบบวงจรรวม ประเภทดังกล่าวเป็นรายแรกและรายเดียวของประเทศไทย นำทีมโดยนักออกแบบผู้มีประสบการณ์จากซิลิคอน วัลเลย์ สหรัฐอเมริกา โดยได้รับความร่วมมือในการผลิตจากโรงงานเจือสารวงจรรวมที่มีขนาดใหญ่และน่าเชื่อถือหลายแห่งทั่วโลก

ด้วยประสบการณ์นับสิบปี บริษัทซิลิคอน คราฟท์ ยังนำเสนอแบบวงจรรวมและ ip cores เพื่อสนับสนุนงานออกแบบ RFID หลากหลายด้าน และยังคงพัฒนาขีดความสามารถในการออกแบบอย่างต่อเนื่อง เพื่อสร้างความได้เปรียบให้กับลูกค้าที่ใช้ผลิตภัณฑ์ของบริษัทฯ ในปีพ.ศ. 2555-2556 บริษัทฯ ได้ขยายขอบเขตการวิจัยและพัฒนาออกไปสู่เรื่อง NFC (Near Field Communication) และวิศวกรรมชีวการแพทย์ ซึ่งเทคโนโลยี

ดังกล่าวมีความสำคัญมากจนอาจเปลี่ยนแปลงวิถีการใช้ชีวิตของมวลมนุษยชาติได้ เช่นการพัฒนาอุปกรณ์ตรวจวัดขนาดพกพาไร้แบตเตอรี่ ใช้งานร่วมกับโทรศัพท์มือถือสมาร์ทโฟน

ปัจจุบันบริษัทฯ ส่งออกผลิตภัณฑ์วงจรรวมหลายสิบล้านชิ้นต่อปี สร้างรายได้รวมกว่า 300 ล้านบาท ด้วยทีม วิศวกรออกแบบประมาณ 60 คน และทีมงานด้านอื่นๆ รวมกันกว่า 110 ชีวิต นอกจากนี้บริษัทฯ ยังให้ความสำคัญอย่างยิ่งในการสร้างบุคลากรทางด้านการออกแบบวงจรรวมและระบบสมองกลฝังตัว เนื่องจากเป็นสาขา ที่ขาดแคลนที่ต้องใช้ความรู้และความพยายามสูง แต่สามารถสร้างมูลค่าเพิ่มให้กับสินค้าได้มากอันเป็นผลดีต่อเศรษฐกิจ ของประเทศ บริษัทจึงให้การส่งเสริมกิจกรรมทางวิชาการอย่างสม่ำเสมอ เช่นความร่วมมือกับสมาคมสมองกลฝังตัว อย่างต่อเนื่อง รับเชิญเป็นวิทยากรพิเศษในวิชาเรียนทางด้านวิศวกรรมไฟฟ้าและคอมพิวเตอร์ รวมถึงการให้ทุนการศึกษา แก่ห้องวิจัยหลายแห่ง เป็นต้น เพราะตระหนักดีว่าบริษัทยังต้องการบุคลากรที่มีความรู้ความสามารถอีกเป็นจำนวนมาก เพื่อที่จะสร้างผลิตภัณฑ์ที่ดียิ่งๆ ขึ้นไป

ขอบเขตงานของบริษัท

บริษัทนี้มีแผนกการทำงานในส่วนของวิศวะทั้งหมด ๓ แผนก

๑. Analog Circuit Design
๒. Embedded System Design
๓. Digital Circuit Design

และเมื่อนำผลลัพธ์ของงานทั้ง ๓ แผนกมารวมกันนั้นจะได้ผลิตภัณฑ์ทั้งหมด ๕ อย่าง

๑. NFC IC
๒. LF Tag IC
๓. HF Tag IC
๔. HF Reader
๕. UHF IC
๖. Demo Kit
๗. ASIC ODM

บทที่ ๓ รายละเอียดของงานที่ทำ

เกริ่นนำ

การฝึกงานในครั้งนี้งานที่ได้รับมีทั้ง 2 สายงาน ทั้ง Analog และ Digital โดยงาน Analog นั้นจะเป็นทำ Two Stages Op Amp ส่วนสายงาน Digital งานที่ได้รับคือการเขียน Code VHDL เพื่อสร้างวงจร Encryption แบบ AES128 และ AES128/256 และโครงงานในฉบับนี้มีการแบ่งงานออกเป็น 2 Part อย่างชัดเจน คือ Two Staged Op Amp และ AES128 and AES128/256 Encryption

Part 1: Two Staged Op Amp

บทนำ

Op Amp นั้นเป็นอุปกรณ์ที่มีประโยชน์มากในแง่ของความสะดวก ดังนั้นการออกแบบ Op Ampนั้นจึงเป็นที่แพร่หลายเป็นอย่างมาก มีรูปแบบอยู่มากมายและหลากหลายวิธีซึ่งจะมีข้อดีข้อเสียแต่ละอย่างที่ต่างกันไป ดังนั้นเราจึงจำเป็นที่จะมีความรู้พื้นฐานเพื่อใช้ในการ trade off ตัวแปรของ Op Amp เพื่อให้ได้ Spec ตามที่เราพึงปราถนา หรือในบางครั้งหากการปรับค่านั้นเป็นไปได้อย่างมาก เราก็จำเป็นที่จะต้องเปลี่ยนเทคนิกหรือผสมผสานเทคนิก เพื่อให้ง่ายต่อการปรับค่า

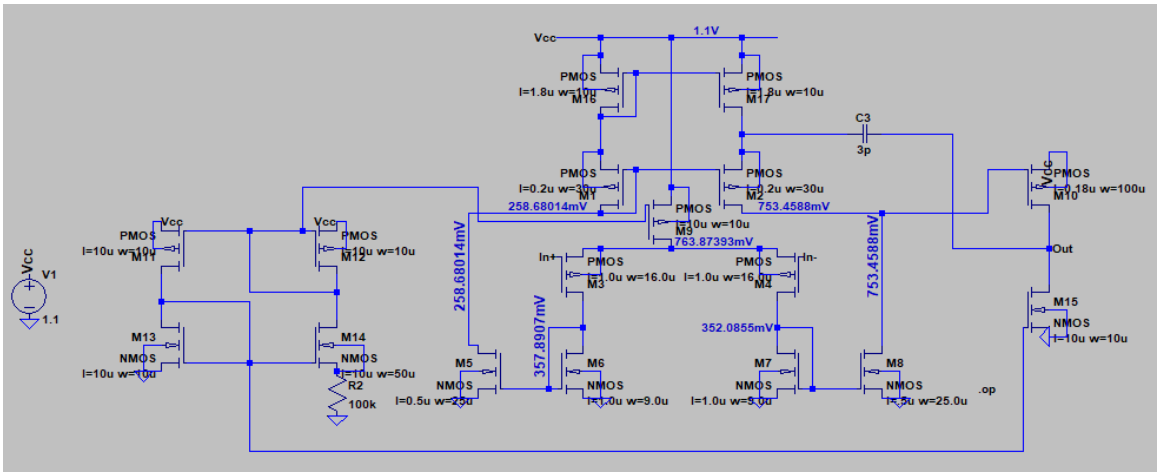


Figure 1

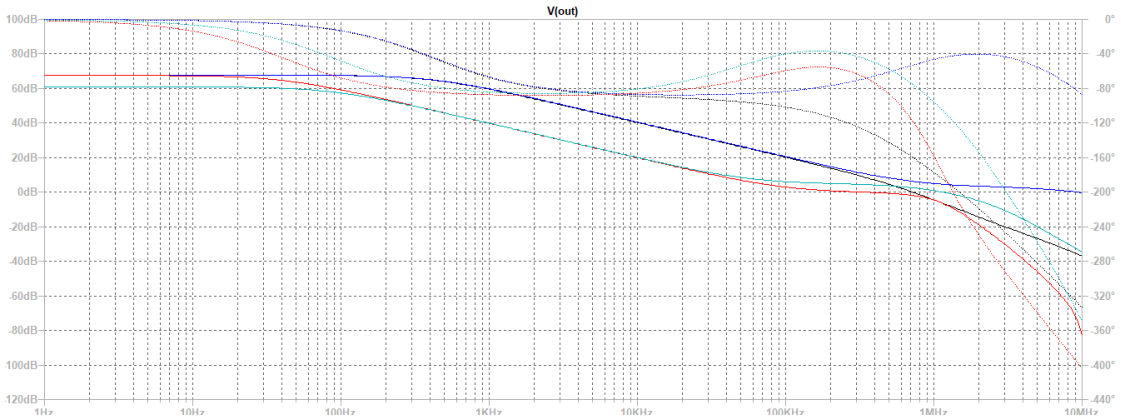


Figure 2

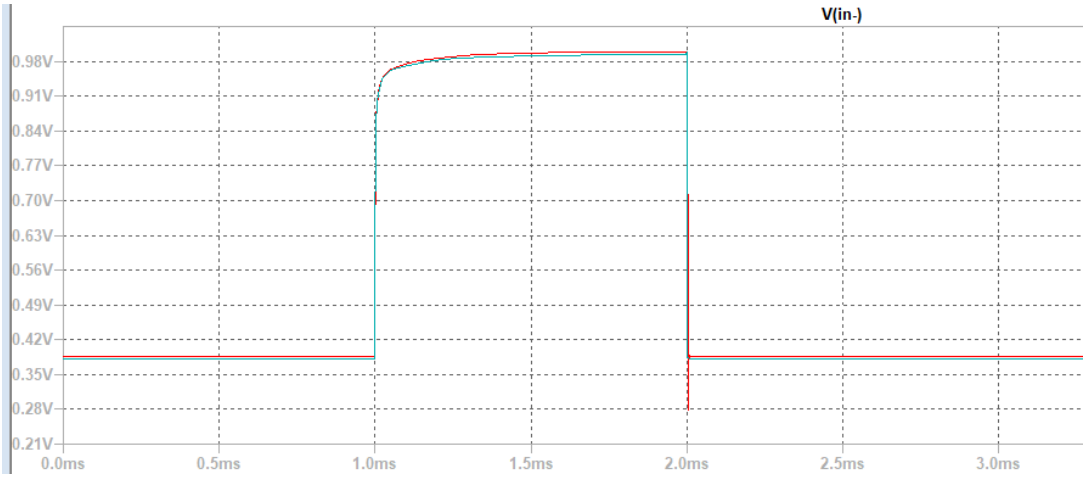


Figure 3

วงจรที่ทำคือการผสมผสานระหว่าง INDIRECT COMPENSATION OPAMP กับ MIRROR OPAMP หรือเรียกได้ว่าเป็นวงจร INDIRECT COMPENSATION MIRROR OPAMP ตาม Figure 1 และลองปรับค่าหลายครั้ง ทำให้ได้ผลลัพธ์เป็นที่ค่อนข้างหน้าพอใจ เพราะว่า Bode Plot ที่ได้เกือบจะผ่าน Spec ที่ได้รับมอบหมาย ในแง่ของ Gain และ Bandwidth ณ ICMR ตาม Figure 2 ที่ต่างไป รวมทั้ง Pulse Response (Figure 3) ด้วย

หลักการที่ถูกใช้ในการปรับนั้นคือ

$$BW = \frac{g_{m1}}{C_c}$$

$$p_2 = \frac{1}{R_c C_1}$$

$$z = \frac{1}{\left(\frac{1}{g_{m6}} - R_c\right) C_c}$$

สรุป

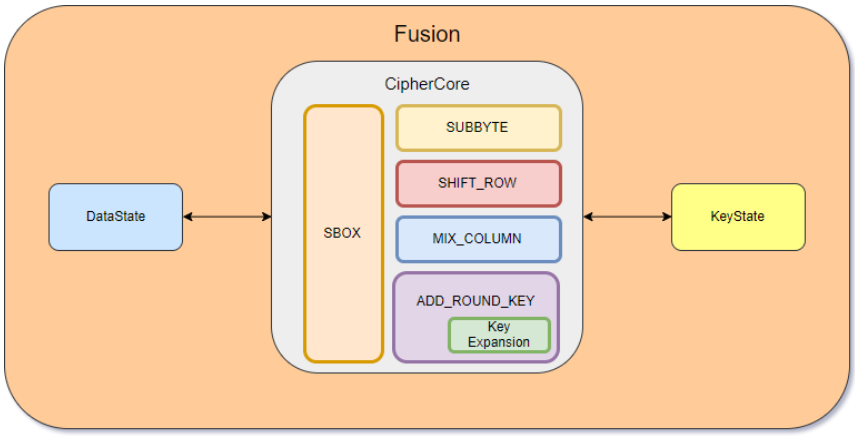
การทำ Analog ในครั้งนี้ ทำให้ทราบว่าในวงการ Analog ความยากอยู่ที่การปรับ เพราะว่า Analog นั้นมีแง่ของ Qualitative ซึ่งต่างจาก Digital ที่มีเพียง Logic 0 หรือ 1 เท่านั้น อย่างไรก็ตามการปรับค่ามันมี Trend ของมันอยู่ หากเราสามารถทราบว่าการปรับค่าอะไร จะส่งผลต่ออะไรแล้วจะทำให้เราสร้างวงจร Analog ได้อย่างไม่ยากลำบาก

Part 2: AES-128, AES-128/256 Comparison

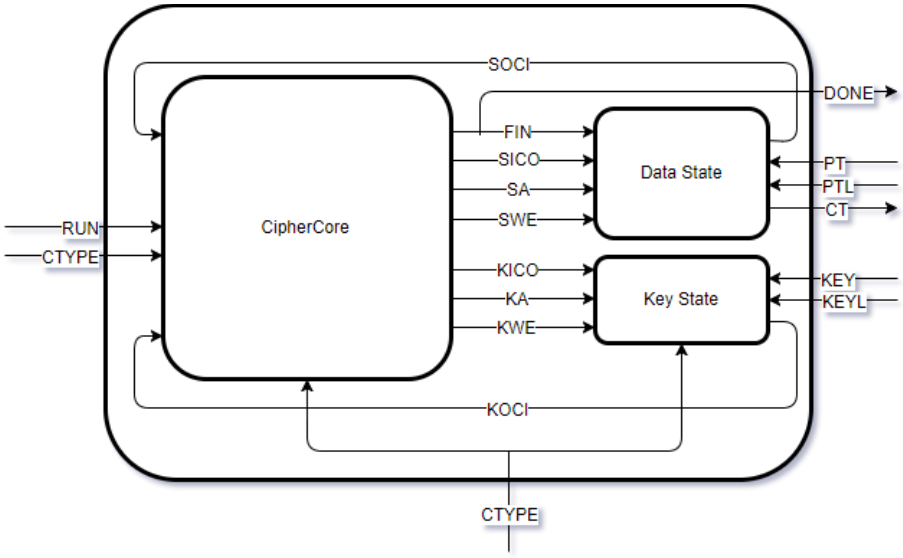
บทนำ

ปัจจุบันนี้มี Super Computer ซึ่งสามารถแกะรหัสอะไรก็ได้ ดังนั้นความปลอดภัยจึงเป็นสิ่งที่ต้องระแวงและระวังเป็นอย่างยิ่ง ดังนั้นรหัสที่มีความซับซ้อนในเชิงโครงสร้างจึงเป็นสิ่งที่จำเป็นอย่างมาก สำหรับ Part นี้จะทำการอธิบายวงจร AES-128 และวงจร AES-128/256 ในรูปแบบ 8 bit แล้วนำมาเปรียบเทียบกันว่า ขนาดและพื้นที่ที่มีเพิ่มเติม มันมากขึ้นเพียงใด

Overall Structure



Top Module Wiring



CipherCore

Top Module Signal

CLK	: in std_logic	: Input Clock
RST	: in std_logic	: Input Reset
RUN	: in std_logic	: Perform Encrypt after load
CTYPE	: in std_logic	: Cipher Type
SOCI	: in std_logic_vector (7 downto 0)	: Data State Out Cipher In
SICO	: out std_logic_vector (7 downto 0)	: Data State In Cipher Out
SA	: out std_logic_vector (3 downto 0)	: State Address
SWE	: out std_logic	: State Write Enable
KOCI	: in std_logic_vector(7 downto 0)	: Key Out Cipher In
KICO	: out std_logic_vector(7 downto 0)	: Key In Cipher Out
KA	: out std_logic_vector(4 downto 0)	: Key Address
KWE	: out std_logic	: Key Write Enable
FIN	: out std_logic	: Cipher Finished

ตัวแปรเกี่ยวกับ State

CipherState : enum : เพื่อชี้ว่า FSM นี้กำลังทำงาน Operation ใดอยู่ โดย State ที่เป็นไปได้คือ (IDLE, SUB_BYTE, SHIFT_ROW, MIX_COLUMN, ADD_ROUND_KEY)

IDLE : State สำหรับการพักและไม่ทำงาน

SUB_BYTE : State ที่ทำการแทนค่าข้อมูลแต่ละตัวลงใน S-BOX

SHIFT_ROW : State ที่ทำการสลับตำแหน่งใน Row

MIX_COLUMN : State ที่ทำการคูณ Matrix ใน Column

ADD_ROUND_KEY : State ที่ทำการ XOR State(Data) ด้วย Key

KeyState : enum : เพื่อชี้ว่าใน Sub-FSM นี้กำลังทำงาน Operation ใดอยู่ ซึ่ง Sub-FSM นี้จะทำงานเฉพาะตอนที่อยู่ในสถานะ ADD_ROUND_KEY เท่านั้น โดย State ที่เป็นไปได้คือ (IDLE, READ_LAST, READ_MIDDLE, CHAIN)

IDLE : State สำหรับการพักและไม่ทำงาน

READ_LAST : State ที่อ่าน Key จาก Column สุดท้าย

READ_MIDDLE : State ที่อ่าน Key จาก Column ที่ 3 (เริ่มต้นจาก 0)

CHAIN : State ที่ทำการ XOR และ Save ข้อมูลทั้ง Key และ State

rwState : enum : เพื่อชี้ว่า FSM นี้อยู่ในกระบวนการไหน READ หรือ WRITE แต่ตัวแปรนี้จะใช้ในเฉพาะบาง CipherState

ตัวแปรเกี่ยวกับ Address ของ State และ Key

StateAddress : unsigned(3) : สำหรับเก็บตัวแปร Address ของ State(Text)

KeyAddress : unsigned(3) : สำหรับเก็บตัวแปร Address ของ Key

StateAddressN : std_logic_vector(3 downto 0) : เป็น Combinational Logic ที่มาจาก RegRow และ RegCol

ตัวแปร Register ที่สำหรับการเก็บข้อมูลชั่วคราว

RegZ : std_logic : ใช้ในการป้องกันการย้าย State เมื่อ StateAddress เป็น 0 ในครั้งแรก

RegA : std_logic_vector(7 downto 0)

RegB : std_logic_vector(7 downto 0)

RegC : std_logic_vector(7 downto 0)

RegD : std_logic_vector(7 downto 0)

ตัวแปรพิเศษสำหรับการทำ Mix Column

SigAx : std_logic_vector(7 downto 0);

SigBx : std_logic_vector(7 downto 0);

SigCx : std_logic_vector(7 downto 0);

SigDx : std_logic_vector(7 downto 0);

SigSOCIx : std_logic_vector(7 downto 0);

ตัวแปรสำหรับนับจำนวนรอบ

Round : unsigned(3 downto 0)

LRound : unsigned(3 downto 0) : ย่อมาจาก Last Round เป็นสัญญาณที่ขึ้นอยู่กับ CT(CipherType)

Substitution Box

SBox : สำหรับใช้ในการแทนค่าตอนทำ Operation Sub Byte และ Add Round Key

Round Constant

RCon : เป็น List ของ Round Constant ที่ใช้ในการ XOR ในแต่ละรอบตอนช่วง Add Round Key

Main State Diagram

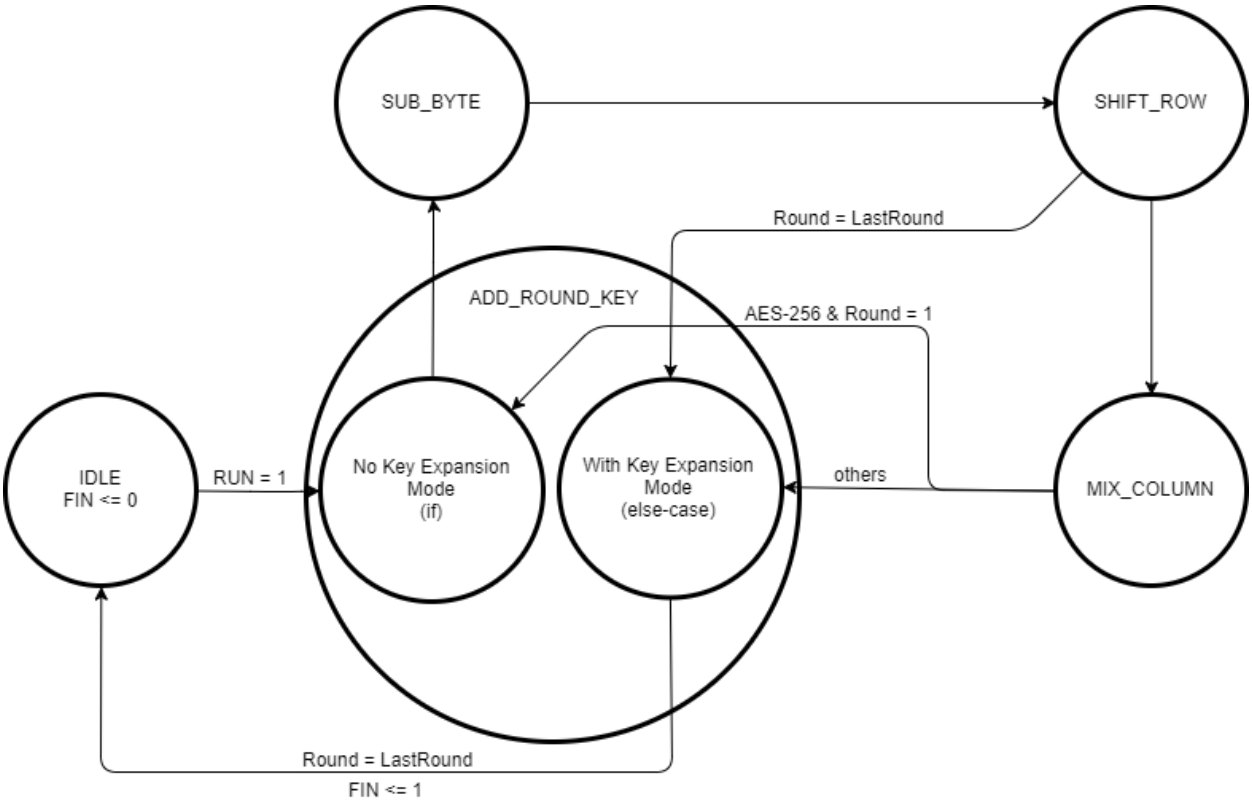


Figure 1

ภาพดังรูป Figure 1 เป็น State Diagram ที่แสดงหลักการทำงาน และจะเริ่มทำงานเมื่อมีการป้อนสั่งคำสั่ง RUN หลังจากนั้น FSM นี้จะวนจาก Add Round Key แล้วต่อด้วย Sub Byte, Shift Row และ Mix Column สุดท้ายกลับไปที่ Add Round Key อีกครั้ง เมื่อทำถึงรอบสุดท้าย FSM นี้จะ Skip คำสั่ง Mix Column และไปทำ Add Round Key หลังจากนั้นก็ส่งสัญญาณ FIN(Finish) เพื่อบอกให้ Data State ทำการป้อนข้อมูล Cipher Text ออกจากตัวมาเป็นอันสิ้นสุดกระบวนการเข้ารหัส AES

Add Round Key(No Key Expansion) State Diagram

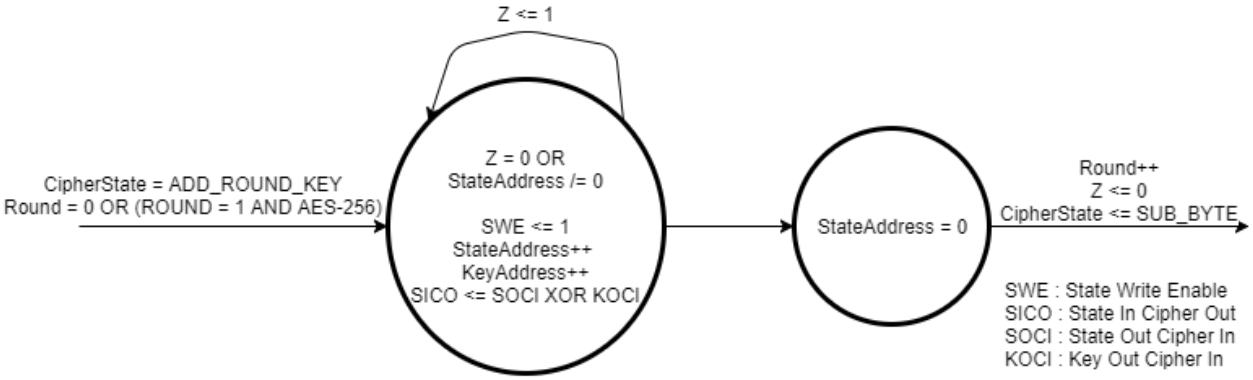


Figure 2

Diagram(Figure 1) นี้แสดงให้เป็นถึง การทำงานของ Add Round Key ซึ่ง Add Round Key ในรอบนี้จะไม่ทำ Key Expansion และจะมีเพียงแค่การนำ Key มา XOR กับ Data State เท่านั้น

Add Round Key (With Key Expansion) State Diagram

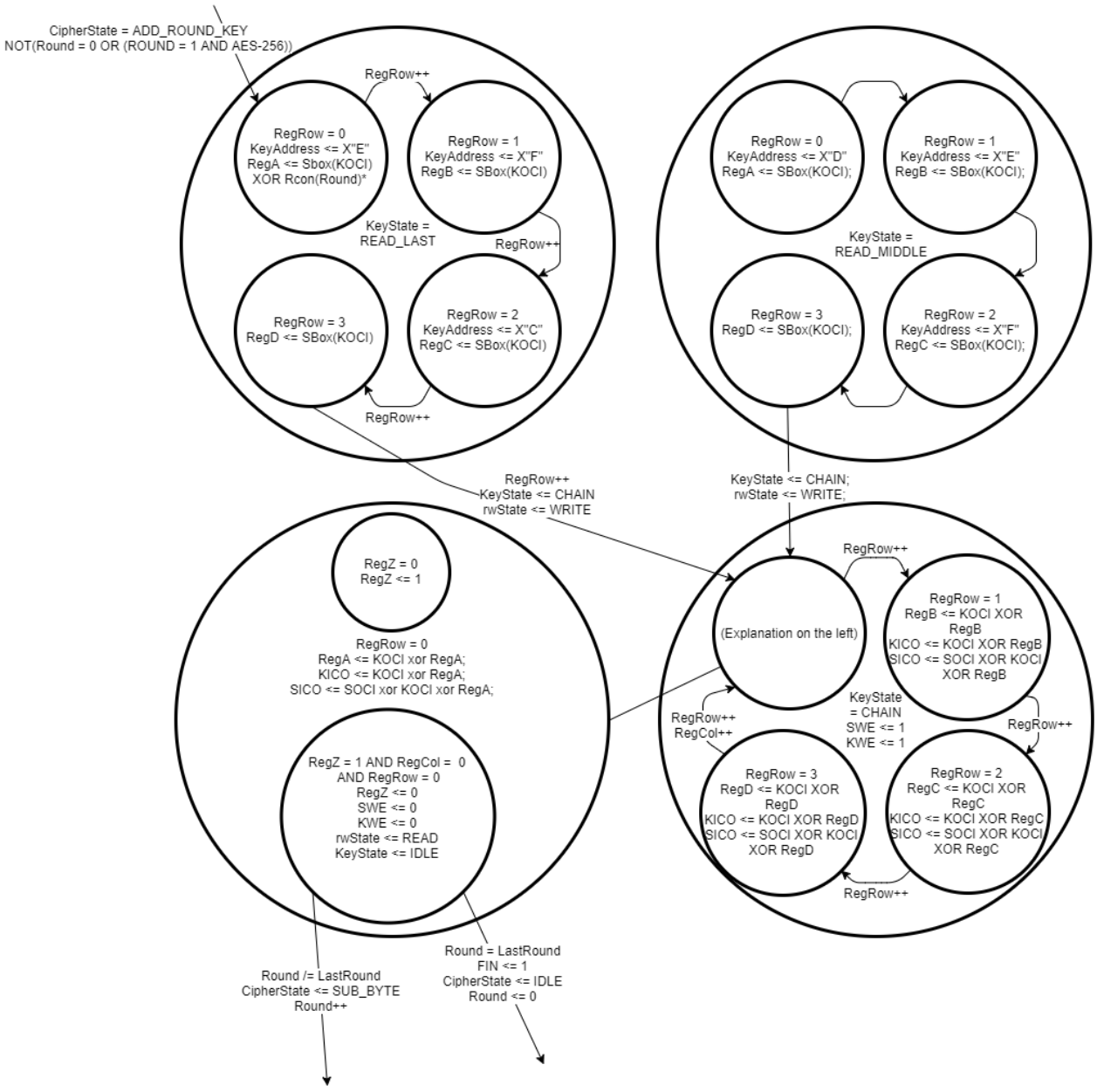


Figure 3

0	4	8	C	<- Read (4)
1	5	9	D	<- Read (1)
2	6	A	E	<- Read (2)
3	7	B	F	<- Read (3)

Figure 4

Diagram ตาม Figure 3 แสดงให้เป็นถึง การทำงานของ Add Round Key โดยที่จะเป็นกรณีทั่วไปโดยจะมีการทำ Key Expansion โดย เริ่มแรกจาก READ LAST คือการอ่านค่าหลักสุดท้ายของ KeyState โดยเลือก Address D, E, F, C (Figure 4) พร้อมแทนค่าลงใน S-BOX และ XOR ด้วย Round Constant แล้วเก็บเข้า RegA, RegB, RegC, RegD ตามลำดับ ซึ่งก็เป็นการสิ้นสุดการทำงานของ READ LAST และพร้อมที่จะทำงานในส่วนของ Key Expansion(CHAIN)

Old KeyState			
K0	K4	K8	KC
K1	K5	K9	KD
K2	K6	KA	KE
K3	K7	KB	KF

Old DataState			
D0	D4	D8	D12
D1	D5	D9	D13
D2	D6	D10	D14
D3	D7	D11	D15

Figure 5

New KeyState			
A XOR K0	K4	K8	KC
B XOR K1	K5	K9	KD
C XOR K2	K6	KA	KE
D XOR K3	K7	KB	KF

New DataState			
A XOR K0 XOR D0	D4	D8	D12
B XOR K1 XOR D1	D5	D9	D13
C XOR K2 XOR D2	D6	D10	D14
D XOR K3 XOR D3	D7	D11	D15

Figure 6

หลังจากที่ได้อ่านค่าหลักสุดท้ายและผ่านกระบวนการต่างๆ ก็มาถึงกระบวนการ Chain คือการนำค่าใน Reg ต่างๆมา XOR กับ KeyState เพื่อสร้าง Key ใหม่สำหรับการ ทำ Key Expansion ครั้งถัดไป และจะเห็นได้ว่า การทำ Key Expansion จะทำควบคู่กับการ Add Round Key หรือก็คือการนำ Key ที่ได้มานั้นมา XOR กับ Data State ไปด้วย(Figure 5, Figure 6)

Key Address(4) = 0				Key Address(4) = 1			
K0	K4	K8	KC	K0	K4	K8	KC
K1	K5	K9	KD	K1	K5	K9	KD
K2	K6	KA	KE	K2	K6	KA	KE
K3	K7	KB	KF	K3	K7	KB	KF

Figure 7

ในกรณี AES-256 Key มีหลักว่าจะต้องนำไปเข้า SBOX ก่อนที่ที่จะเข้า Key Expansion ต่อไป ซึ่งจากการสังเกตุนั้น รอบที่เป็นรอบคู่ (Round = 0,2,4,6) จะใช้ Key Address ชุดซ้าย ส่วนรอบคี่จะใช้ Key Address ชุดขวา จึงจำเป็นที่จะต้องมีกระบวนการ Read Middle เพื่อทำการแทนค่าลง S-BOX และนำใส่เข้า RegA, RegB, RegC, RegD หลังจากนั้นก็เข้ากระบวนการ CHAIN ต่อไป

Sub Byte State Diagram

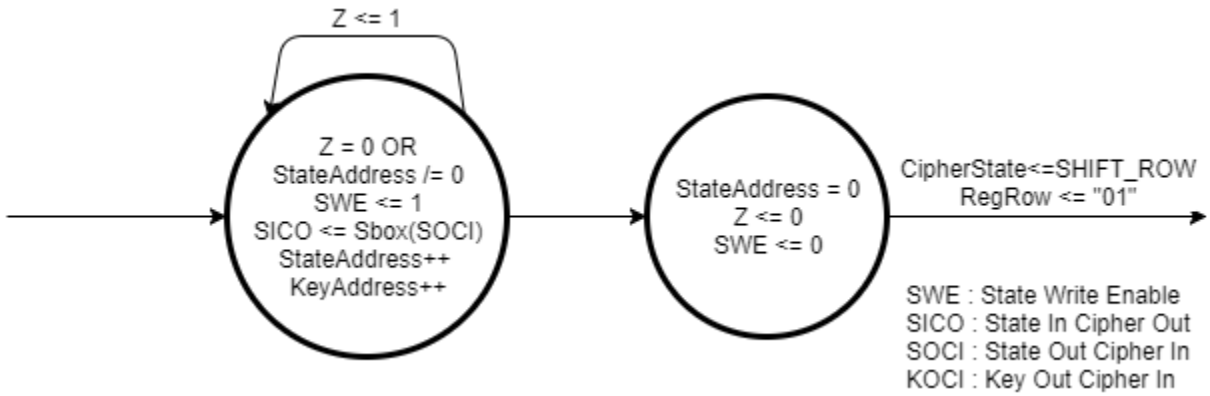


Figure 8

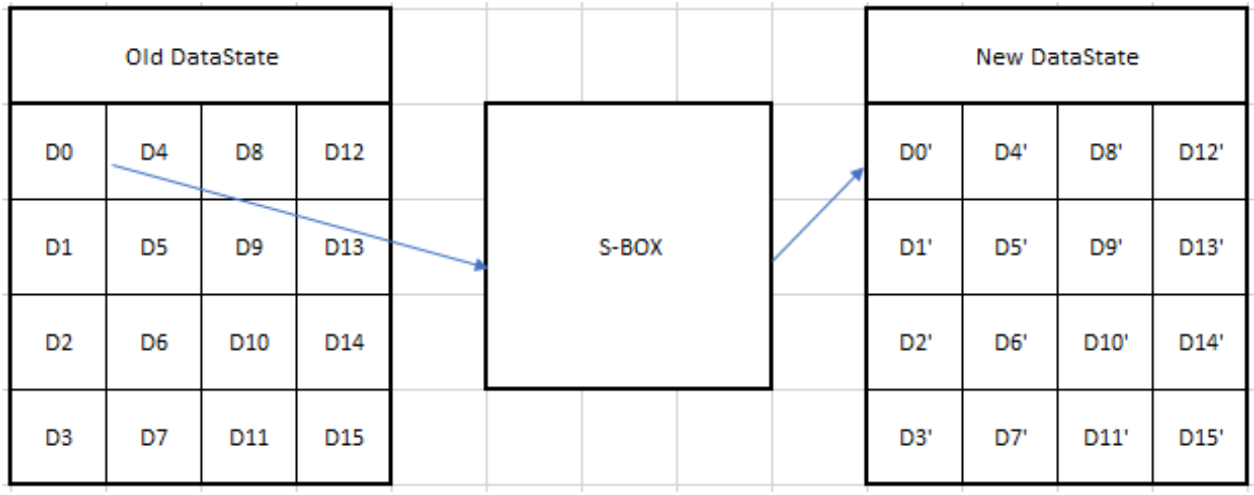


Figure 9

State Sub Byte คือการแทนค่า Data แต่ละตัวลงใน S-Box ดัง Figure 9 แล้วนำบันทึกใส่ Data State อีกที การกระทำนี้จะใช้เพียง 1 Clock ต่อ 1 Bit ตามที่ได้อธิบายโครงสร้างของ Data State การบันทึกจะบันทึกใส่ที่ Address – 1 ทำให้การ Read และการ Write พร้อมกันนั้นเป็นไปได้ FSM นี้จะเปลี่ยน State เมื่อ State นั้นได้แทนค่าครงทุกตัวแล้ว หรือเรียกได้ว่า State Address นั้นกลับไปที่จุดเริ่มต้น ดังนั้นมันจึงมีความจำเป็นที่จะต้องใช้ Register Z เพื่อให้ไม่มีการย้าย State เมื่อ State Address = 0 ในครั้งแรก

Shift Row State Diagram

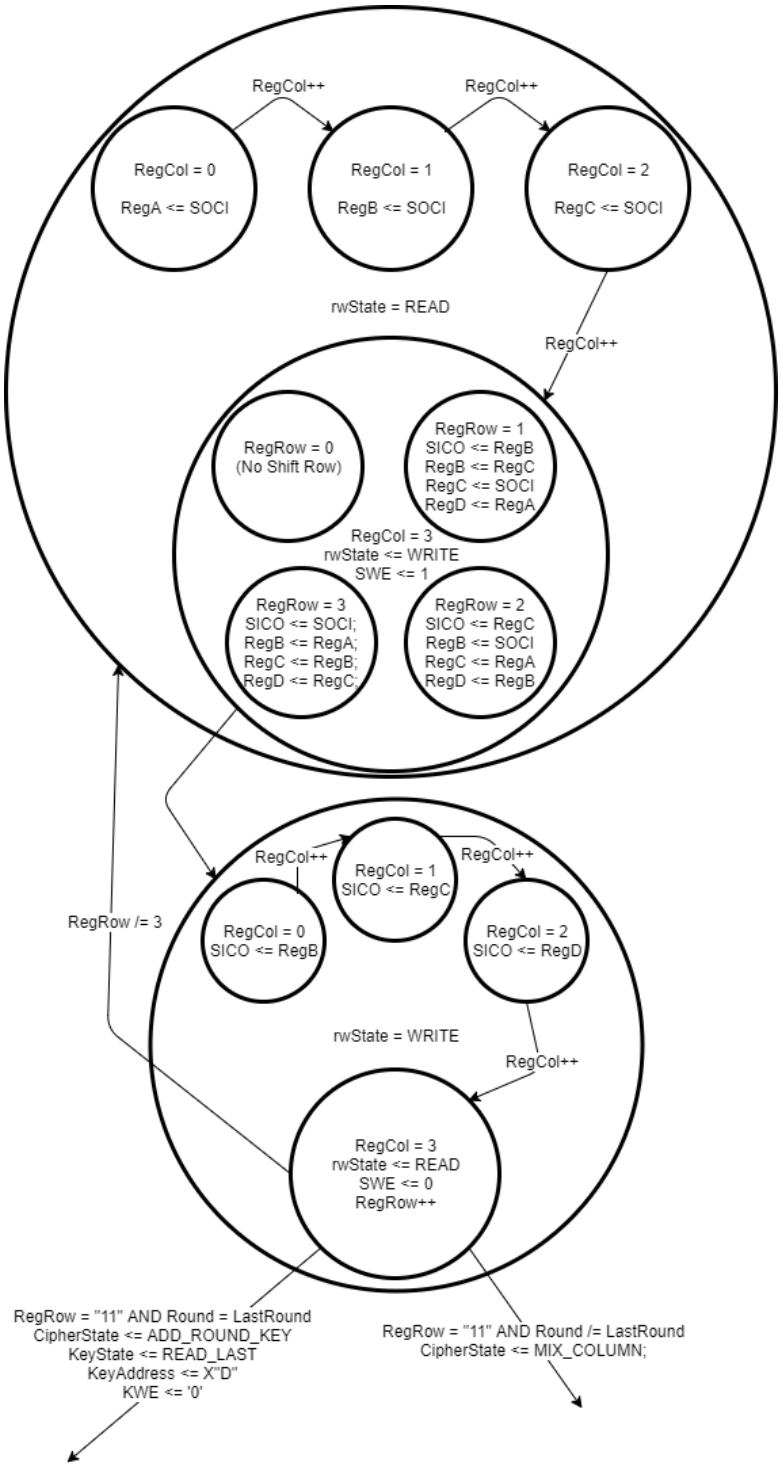


Figure 10

Old DataState			
D0	D4	D8	D12
D1	D5	D9	D13
D2	D6	D10	D14
D3	D7	D11	D15

New DataState			
D0	D4	D8	D12
D5	D9	D13	D1
D10	D14	D2	D6
D15	D3	D7	D11

Figure 11

State Shift Row นั้นเป็นการสลับตำแหน่งในแถวเดียวกันตาม Figure 11 ซึ่งแต่ละแถวจะมีลักษณะที่สลับในรูปแบบที่ต่างกัน เนื่องจากมีการ Operate แบบ 8 bit ดังนั้นขั้นตอนที่ FSM ดัง Figure 10 นี้ทำคือ เปลี่ยน Column (การเขียนหรืออ่าน Address ใน State นี้จะเกิดจาก Combinational Logic ของ Row และ Column) ในขั้นเริ่มต้นจะทำการอ่านค่าทีละ Address ใส่ใน Register ต่างๆ หลังจากนั้นก็ทำการสลับตำแหน่งใน Register พร้อมทำการส่งค่าออก ไปเรื่อยๆ เมื่อส่งเรียบร้อยก็จะเพิ่มค่า Row ขึ้นอีก 1 แล้วกลับไปอ่านแต่ละ Column อีกที และเมื่อ Row มีค่าเป็น 3 แล้วก็ทำการเปลี่ยน Operation ซึ่ง Operation ที่จะทำต่อนั้นขึ้นอยู่กับว่า รอบของ FSM หลักนั้นถึงรอบสุดท้ายแล้วหรือไม่ หากใช่ก็ต้องไปทำ Add Round Key ต่อไป ในทางกลับกัน หากไม่ใช่ก็ FSM ก็จะไปทำในส่วนของ Mix Column

Mix Column State Diagram

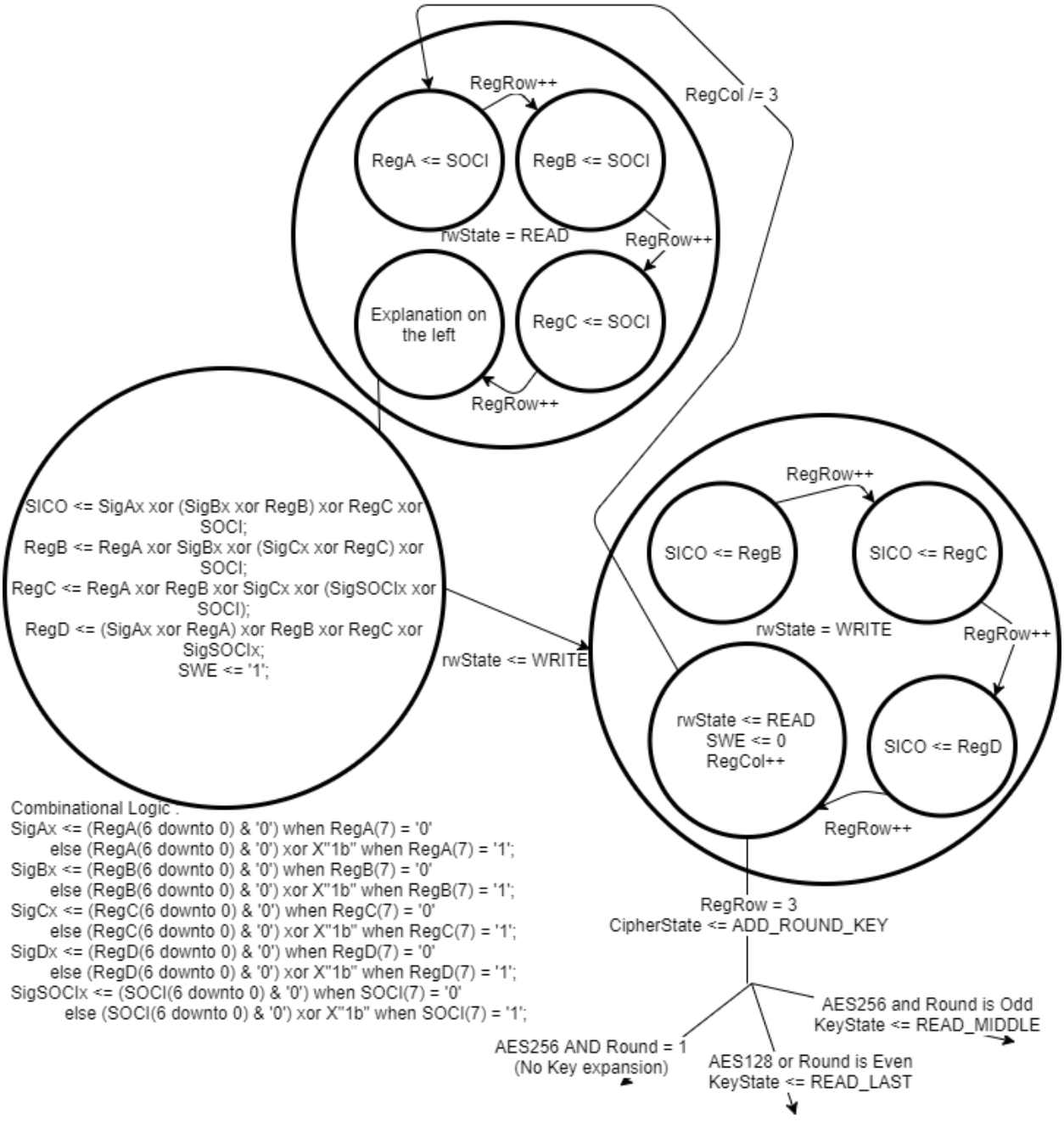


Figure 12

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Mix Column นั้นเป็นการผสมข้อมูลทาง Column โดยตามหลักจะเป็นคูณ Matrix 4x4 ตาม สมการด้านบน แต่ใน Code VHDL จะเป็นการทำ Combination Logic และผลลัพธ์ที่ได้จะเป็นผลของการ Shift และพิจารณาในรูปแบบของ GF(8) ซึ่งมีหลักการดังนี้ ยกตัวอย่างเช่นการหาผลลัพธ์ของ b_0 จะได้ว่า

$$b_0 = 2a_0 \oplus 3a_1 \oplus a_2 \oplus a_3$$

$2a_0$ เป็นการคูณ 2 ทาง GF(8) ถ้าหากว่า

MSB ของ $a_0 = 0$, a_0 จะมีค่าเป็น a_0 ที่ Left Shift ไป 1 ครั้ง เช่น

ตอนแรก $a_0 = 01110111$ ตอนหลัง $a_0 = 11101110$

ในทางกลับกัน MSB ของ $a_0 = 1$, a_0 จะต้องทำการ XOR กับ 00011011 หลังจากที่ Left Shift ไปแล้ว 1 ครั้ง เช่น

ตอนแรก $a_0 = 11101110$ หลัง Left Shift ได้ $a_0 = 11011100$

และ $XOR\ 00011011$ จะได้ $a_0 = 11000111$

$3a_1$ เป็นการคูณ 3 ทาง GF(8) วิธีการคูณจะเป็นดังนี้

$$3 \times x = (2 \oplus 1) \times x = (2 \times x) \oplus x$$

จะเห็นได้ว่ามันคือการทำ $2a_1$ และ $XOR\ a_1$

ในบรรทัด SigAx <= (RegA(6 downto 0) & '0') when RegA(7) = '0' else (RegA(6 downto 0) & '0') xor X"1b" when RegA(7) = '1'; เป็น Combinational Logic ที่ใช้ในการอธิบายการกระทำเช่นนี้

Simulation AES-128

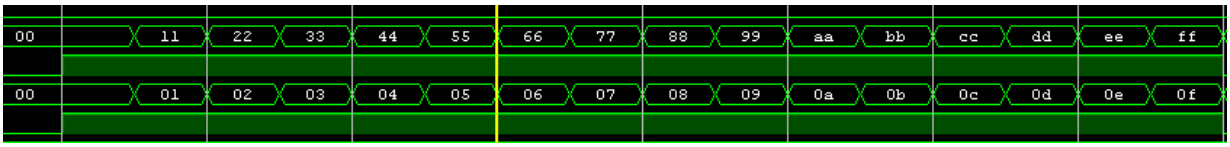
From Reference (Plain Text, Key)

C.1 AES-128 (*Nk*=4, *Nr*=10)

PLAINTEXT: 00112233445566778899aabbccddeeff
KEY: 000102030405060708090a0b0c0d0e0f

round[10].output 69c4e0d86a7b0430d8cdb78070b4c55a

Input (Plain Text, Key)



Output

ซึ่งได้ผลลัพธ์ที่ตรงกับความคาดหวัง

Simulation AES-256

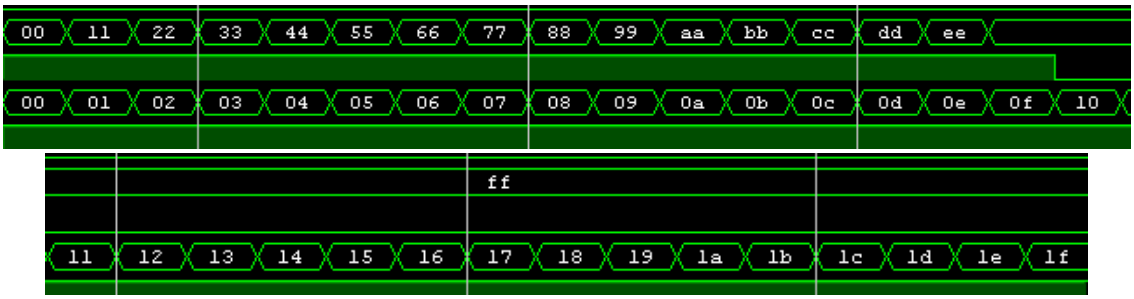
From Reference (Plain Text, Key)

C.3 AES-256 (*Nk*=8, *Nr*=14)

```
PLAINTEXT:  00112233445566778899aabbccddeeff
KEY:        000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f

round[14].output    8ea2b7ca516745bfeafc49904b496089
```

Input (Plain Text, Key)



Output

ซึ่งได้ผลลัพธ์ที่ตรงกับความคาดหวัง

AES-128 vs AES-128/256 Comparison

AES-128

Name	Slice LUTs (63400)	Slice Registers (126800)	F7 Muxes (31700)	F8 Muxes (15850)	Slice (1585 0)	LUT as Logic (63400)	LUT as Memory (19000)	LUT Flip Flop Pairs (63400)	Bonded IOB (210)	BUFGCTRL (32)
Fusion	422	98	56	16	119	382	40	79	31	1
Cipher (CipherCore)	308	81	56	16	106	308	0	74	0	0
DState (State)	63	13	0	0	20	39	24	3	0	0
KState (KeyState)	51	4	0	0	14	35	16	2	0	0

AES-128/256

Name	Slice LUTs (63400)	Slice Registers (126800)	F7 Muxes (31700)	F8 Muxes (15850)	Slice (1585 0)	LUT as Logic (63400)	LUT as Memory (19000)	LUT Flip Flop Pairs (63400)	Bonded IOB (210)	BUFGCTRL (32)
Fusion	563	355	61	24	218	539	24	81	31	1
Cipher (CipherCore)	341	81	29	8	131	341	0	74	0	0
DState (State)	64	13	0	0	20	40	24	3	0	0
KState (KeyState)	158	261	32	16	125	158	0	3	0	0

จะเห็นได้ว่าสิ่งที่เพิ่มเติมมาอย่างชัดเจนคือ KeyState นั้นมี slice เพิ่มจำนวนมาเป็น 3 เท่า

สรุป

วงจร AES Encrypt นั้นเป็นวงจรที่ไม่ซับซ้อน แต่มีหลายขั้นตอน ซึ่งในความเป็นจริงแล้ววงจร Digital ทั่วไปสามารถอนุมานเป็นรูปแบบนี้ได้ทั้งนั้น และสำหรับความเห็นของผู้จัดทำนั้น Digital นั้นมักจะเป็นการคิด Logic ไปเรื่อยๆ แต่ Analog นั้นมักจะเป็นการปรับค่าให้ได้ตาม Specification โดยที่การปรับค่านั้น เราจะต้องเข้าใจถึงอุปกรณ์เชิงลึกอย่างถ่องแท้

อ้างอิง

http://dvt.sisat.ac.th/home/index.php?option=com_content&view=article&id=54&Itemid=61

https://crypto.stackexchange.com/questions/2402/how-to-solve-mixcolumns

http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

NIST.FIPS.197 - nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

SIC_Lecture.pdf

ภาคผนวก

ศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Placement Service Centre, Faculty of Engineering, Chulalongkorn University
ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทร. 0-2218-6303 โทรสาร 0-2252-2687

รายงานการฝึกงานทุกสองสัปดาห์
ฉบับที่...1....

ชื่อ-สกุล นริศร์ หนังสือ เลขประจำตัว 5730281021 ภาควิชาวิศวกรรม ไฟฟ้า
ชื่อหน่วยงาน Silicon Craft
ที่อยู่โดยละเอียด 3rd FL., Le Unique Plaza No. 40 Thetsaban rangsannua Rd., Ladyao, Chatuchak, Bangkok 10900 Thailand

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ลงชื่อนิสิต
29/5/60	8	Basic Electronic Lesson ครั้งที่ 1	นริศร์
30/5/60	8	» ครั้งที่ 2	นริศร์
31/5/60	8	» ครั้งที่ 3	นริศร์
1/6/60	8	» ครั้งที่ 4	นริศร์
2/6/60	8	» ครั้งที่ 5	นริศร์
5/6/60	8	» ครั้งที่ 6	นริศร์
6/6/60	8	Op Amp Design ครั้งที่ 1	นริศร์
7/6/60	8	» ครั้งที่ 2	นริศร์
8/6/60	8	» ครั้งที่ 3	นริศร์
9/6/60	8	» ครั้งที่ 4	นริศร์
12/6/60	8	» ครั้งที่ 5	นริศร์
13/6/60	8	» ครั้งที่ 6	นริศร์
จำนวนชั่วโมงฝึกงานรวมในรายงานฉบับนี้	80	ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ ลงชื่อ.....วิศวกรผู้ควบคุม (.....) ตำแหน่ง MTS วัน/เดือน/ปี 12/6/2017	
จำนวนชั่วโมงฝึกงานในรายงานฉบับก่อน	—		
จำนวนชั่วโมงฝึกงานรวมทั้งหมด	80		

หมายเหตุ นิสิตต้องส่งรายงานฉบับนี้ถึงศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ ทุกสองสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้ เพื่อทำรายงานฉบับสมบูรณ์

แบบฟอร์ม EP-02

ศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Placement Service Centre, Faculty of Engineering, Chulalongkorn University
ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทร. 0-2218-6303 โทรสาร 0-2252-2667

รายงานการฝึกงานทุกสองสัปดาห์
ฉบับที่ 2

ชื่อ-สกุล นริศรา แข็งขัน เลขประจำตัว 5730289021 ภาควิชาวิศวกรรม ไฟฟ้า
ชื่อหน่วยงาน Silicon Craft
ที่อยู่โดยละเอียด 3rd Fl, La Unique Plaza, No 40 Thetsaban rangsannua Rd Ladyao, Chatuchak Bangkok 10900 Thailand.

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ลงชื่อนิสิต
12/6/60	9	Op Amp Design #7	นริศรา
13/6/60	9	Op Amp Design #8	นริศรา
14/6/60	8	Op Amp Design #9	นริศรา
15/6/60	5	Op Amp Design #10	นริศรา
16/6/60	8	Op Amp Design #11	นริศรา
19/6/60	8	Op Amp Design #12	นริศรา
20/6/60	8	Op Amp Design #13	นริศรา
21/6/60	8	Op Amp Design #14	นริศรา
22/6/60	8	Op Amp Design #15	นริศรา
23/6/60	8	Op Amp Design #16	นริศรา

จำนวนชั่วโมงฝึกงานรวมในรายงานฉบับนี้	75
จำนวนชั่วโมงฝึกงานในรายงานฉบับก่อน	80
จำนวนชั่วโมงฝึกงานรวมทั้งหมด	155

ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ

ลงชื่อ ..... วิศวกรผู้ควบคุม
(.....)
ตำแหน่ง ผู้ช่วยผู้จัดการฝ่ายเทคนิค
วัน/เดือน/ปี 28 มิ.ย. 2560

หมายเหตุ นิสิตต้องส่งรายงานฉบับนี้ถึงศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ ทุกสองสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้ เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Placement Service Centre, Faculty of Engineering, Chulalongkorn University
ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทร. 0-2218-6303 โทรสาร 0-2252-2687

รายงานการฝึกงานทุกสองสัปดาห์
ฉบับที่...3....

ชื่อ-สกุล นวิศ์ เผือสอ เลขประจำตัว 5730285021 ภาควิชาวิศวกรรม ไฟฟ้า
ชื่อหน่วยงาน SiliconCraft
ที่อยู่โดยละเอียด 3rd FL., La Unique Plaza No.40 Thetsabanrangsan Rd., Ladyao, Chatuchak, Bangkok 10900 Thailand

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ลงชื่อนิสิต
27/6/60	8	Op Amp Design	นวิศ์
28/6/60	8	Op Amp Design	นวิศ์
29/6/60	8	AES Encryption	นวิศ์
30/6/60	8	AES Encryption	นวิศ์
4/7/60	8	AES Encryption	นวิศ์
5/7/60	8	AES Encryption	นวิศ์
6/7/60	8	AES Encryption	นวิศ์
7/7/60	8	AES Encryption	นวิศ์

จำนวนชั่วโมงฝึกงานรวมในรายงานฉบับนี้	64
จำนวนชั่วโมงฝึกงานในรายงานฉบับก่อน	75
จำนวนชั่วโมงฝึกงานรวมทั้งหมด	219

ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ

ลงชื่อ.....วิศวกรผู้ควบคุม
(ศิรา ตันติรังสี)
ตำแหน่ง Senior Engineer
วัน/เดือน/ปี 12/7/17

หมายเหตุ นิสิตต้องส่งรายงานฉบับนี้ถึงศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ ทุกสองสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้ เพื่อทำรายงานฉบับสมบูรณ์

แบบฟอร์ม EP-02

ศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Placement Service Centre, Faculty of Engineering, Chulalongkorn University
ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทร. 0-2218-6303 โทรสาร 0-2252-2687

รายงานการฝึกงานทุกสองสัปดาห์
ฉบับที่ 4

ชื่อ-สกุล นริศร์ พงษ์ดี เลขประจำตัว 5730289021 ภาควิชาวิศวกรรม ไฟฟ้า
ชื่อหน่วยงาน Silicon Craft
ที่อยู่โดยละเอียด 3rd FL, La Unique Plaza No.40 Thetsabanrangsannua Rd., Ladyao, Chatuchak, Bangkok 10900 Thailand

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ลงชื่อนิสิต
12/7/60	3	VHDL Basics	นริศร์
13/7/60	8	VHDL Basics	นริศร์
14/7/60	8	Soft Skill Training	นริศร์
17/7/60	8	AES-SHIFT Row	นริศร์
18/7/60	8	AES-SUB BYTE	นริศร์
19/7/60	8	AES-MIX COLUMN	นริศร์
20/7/60	8	AES-ADD ROUND KEY	นริศร์
21/7/60	3	AES 256 Upgrade	นริศร์

จำนวนชั่วโมงฝึกงานรวมในรายงานฉบับนี้	54
จำนวนชั่วโมงฝึกงานในรายงานฉบับก่อน	64
จำนวนชั่วโมงฝึกงานรวมทั้งหมด	273

ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ

ลงชื่อ.....วิศวกรผู้ควบคุม
(ศิระ ตันติรังษี)
ตำแหน่ง.....
วัน/เดือน/ปี 21/7/17

หมายเหตุ นิสิตต้องส่งรายงานฉบับนี้ถึงศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ ทุกสองสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้ เพื่อทำรายงานฉบับสมบูรณ์

ศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
Placement Service Centre, Faculty of Engineering, Chulalongkorn University
ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพฯ 10330 โทร. 0-2218-6303 โทรสาร 0-2252-2687

รายงานการฝึกงานทุกสองสัปดาห์
ฉบับที่ 5

ชื่อ-สกุล นายนริศร์ พิงรัก รหัสประจำตัว 5730289021 ภาควิชาวิศวกรรม โยธา
ชื่อหน่วยงาน Silicon Craft
ที่อยู่โดยละเอียด 3rd FL, La Unique Plaza No.210 Thetsabanrangrua Rd., Ladyao, Chatuchak, Bangkok 10900 Thailand

วัน/เดือน/ปี	จำนวนชั่วโมง	งานที่ปฏิบัติโดยย่อ	ลงชื่อนิสิต
24/7/60	9	Presentation	นริศร์
25/7/60	9	อ่านงาน IEEE	นริศร์
26/7/60	8	ทำ Document	นริศร์
27/7/60	8	ทำ Document	นริศร์

จำนวนชั่วโมงฝึกงานรวมในรายงานฉบับนี้	32
จำนวนชั่วโมงฝึกงานในรายงานฉบับก่อน	54
จำนวนชั่วโมงฝึกงานรวมทั้งหมด	305

ขอรับรองว่ารายงานฉบับนี้เป็นความจริงทุกประการ

ลงชื่อ.....วิศวกรผู้ควบคุม
(นาย ภัทธีรวงศ์)
ตำแหน่ง.....
วัน/เดือน/ปี 27/7/17

หมายเหตุ นิสิตต้องส่งรายงานฉบับนี้ถึงศูนย์บริการจัดหางาน คณะวิศวกรรมศาสตร์ ทุกสองสัปดาห์อย่างเคร่งครัด อย่าลืมถ่ายสำเนาเก็บไว้ เพื่อทำรายงานฉบับสมบูรณ์

แบบฟอร์ม EP-02