บทความวิจัย

การประชุมวิชาการวิศวกรรมศาสตร์และเทคโนโลยี มทร.พระนคร ครั้งที่ 4

Proceedings of the 4th RMUTP Conference on Engineering and Technology

การออกแบบวงจรเข้ารหัสด้วยอัลกอริทึมโบลว์ฟิชขนาด 32 บิต
Design of a 32-bit Blowfish Based Encryption Processor

คุณากร ดิษฐโรจน์ และอริยะ ลักษณะสุต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

1381 ถนนประชาราษฎร์ 1 แขวงวงศ์สว่าง เขตบางซื่อ กรุงเทพมหานคร E-mail: {kunakorn-d, aussawin-m}@rmutp.ac.th

บทคัดย่อ

วงจรเข้ารหัสด้วยอัลกอริทึมโบลว์ฟิช(Blowfish)[1] ซึ่งเป็นอัลกอริทึมที่มีความปลอดภัยสูงแต่มีความซับซ้อนต่ำ ทำให้วงจรมีความเร็วในการประมวลผล การศึกษาวิจัยนี้ได้ทำการออกแบบวงจรเอฟพีจีเอเพื่อเข้ารหัสสัญญาณขนาด 32 บิตด้วยอัลกอริทึมโบลว์ฟิช โดยใช้ภาษาอธิบายฮาร์ดแวร์ Verilog ผู้ดำเนินโครงการได้ทดสอบการทำงานระดับอัลกอริทึมด้วยโปรแกรม MATLAB และทดสอบฟังก์ชันการทำงานของฮาร์ดแวร์ที่ได้ออกแบบด้วยโปรแกรม ModelSim แล้วจึงสังเคราะห์วงจรในรูปแบบเอฟพีจีเอบนบอร์ดทดลองรุ่น WARRIOR CYCLONE3-EB02 ด้วย Quartus II ผลการทำงานของฮาร์ดแวร์จริงถูกยืนยันด้วยวงจรถอดรหัสโบลว์ฟิชซึ่งจะให้ค่าสัญญาณเดิมออกมาอย่างถูกต้อง

คำสำคัญ: การเข้ารหัสโบลว์ฟิช เอฟพีจีเอ ภาษาอธิบายฮาร์ดแวร์

Abstract

Blowfish encryption has been well known for its low complexity that can be used in implementing high-performance encryption circuits. This study proposes a design of 32-bit Blowfish based encryption processor using FPGA by Verilog HDL. Our design was functionally verified at algorithm and circuit levels by MATLAB and ModelSim, respectively. The design was synthesized by Quartus II into the FPGA chip on WARRIOR CYCLONE3-EB02 board, and the encrypted result was successfully tested by the decryption circuit where the original word was accurately achieved.

Keywords: Blowfish encryption, FPGA, Hardware Description Language

1. บทนำ

เนื่องจากในปัจจุบันเทคโนโลยีได้มีการพัฒนามากขึ้น จึงส่งผลให้จำเป็นต้องมีการเพิ่มความปลอดภัยในการใช้งานในด้านต่าง ๆ เช่น ด้านความปลอดภัยของข้อมูล เป็นต้น ซึ่งมีความมีความจำเป็นอย่างยิ่งสำหรับป้องกันมิให้ข้อมูลถูกเผยแพร่สู่สาธารณะ จากการค้นคว้าข้อมูลเพิ่มเติมจึงพบว่ามีวิธีการต่าง ๆ หลากหลายวิธีเพื่อป้องกันข้อมูลไม่ให้ถูกเผยแพร่สู่สาธารณะ ในที่นี้จึงได้เลือกวิทยาการเข้ารหัสลับมาประยุกต์เพื่อแก้ไขปัญหาข้างต้น

วิทยาการเข้ารหัสลับ(Cryptography) Crypto แปลว่า “การซ่อน” ส่วน Graph แปลว่า “การเขียน” Cryptography จึงมีความหมายว่า “การเขียนเพื่อซ่อนข้อมูล” เป็นระบบการรักษาความปลอดภัยที่ประกอบด้วย การเข้ารหัส(Encryption) หมายถึง กระบวนการหรือขั้นตอนในการเข้ารหัสข้อมูลที่มีการเปลี่ยนแปลงไปจากเดิม การถอดรหัสข้อมูล(Decryption) หมายถึง กระบวนการหรือขั้นตอนในการถอดรหัสข้อมูล เพื่อให้ข้อมูลที่เข้ารหัสไว้คืนสู่สภาพเดิมก่อนเข้ารหัส เมื่อได้ศึกษาเพิ่มเติมเกี่ยวกับวิทยาการเข้ารหัสลับจึงได้มีการนำอัลกอริทึมโบลว์ฟิชมาใช้ในการเข้ารหัสข้อมูล ซึ่งโบลว์ฟิชเป็นการเข้ารหัสวิธีหนึ่งซึ่งใช้วิธีการเข้ารหัสแบบบล็อก (Block Cipher) และคีย์แบบสมมาตร (Symmetric Key) ซึ่งได้รับการออกแบบในปี ค.ศ. 1993 โดยนายบรูค ชไนย์เออร์ (Bruce Schneier) และการเข้ารหัสแบบโบลว์ฟิชนี้ได้รับความนิยมเป็นอย่างยิ่งในการนำมาใช้ทางด้านการเข้ารหัสกับผลิตภัณฑ์ของซอฟต์แวร์ต่าง ๆ ทั้งยังยากต่อการโจมตีและถูกเจาะวิเคราะห์จาก Cryptanalysis

เนื่องจากเหตุผลที่กล่าวมาในข้างต้นจึงได้มีแนวคิดเพื่อที่จะศึกษาและออกแบบวงจรเข้ารหัสและถอดรหัสด้วยอัลกอริทึมโบลว์ฟิชขนาด 32 บิต โดยศึกษาอัลกอริทึมโบลว์ฟิชด้วยโปรแกรม Matlab ออกแบบวงจรด้วย Verilog HDL และทดสอบการทำงานด้วย ModelSim และ FPGA

2. ทฤษฎีที่เกี่ยวข้อง

2.1 โบลว์ฟิช

โบลว์ฟิชใช้วิธีการเข้ารหัสแบบบล็อกและคีย์แบบสมมาตร โดยการแบ่ง variable-length key โดยมีขนาดความยาว32บิต โบลว์ฟิชเป็นอัลกอริทึมที่มีความรวดเร็วในการทำงาน มีขนาดเล็กกระทัดรัด ไม่ได้จดสิทธิบัตร โบลว์ฟิชวนรอบ 17 ครั้ง มีความเร็วในการทำงานสูง ออกแบบรองรับหน่วยประมวลผลขนาด 32

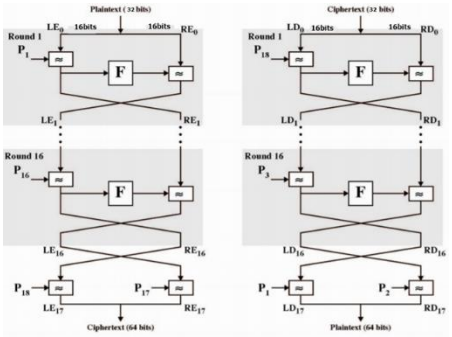
ทำการสลับคีย์17รอบ คีย์ทางซ้ายแต่ละรอบจะผ่านฟังก์ชั่นเอฟ ฟังก์ชั่นเอฟจะมีเอสบล็อกที่มีลอจิกเกต เช่น AND,OR,XOR, ETC. ช่วยเพิ่มความซับซ่อนเพิ่มมากขึ้นจากนั้นสำหรับ i = 1 ถึง 17:

$$xl = F(xr) XOR\ xl\ XOR\ Pi + 1 \qquad (1)$$

$$xr = F(xl) XOR\ xl\ XOR\ Pi \qquad (2)$$

หลังจากรอบที่สิบเจ็ดสลับ xL และ xR อีกครั้งเพื่อยกเลิกการสลับครั้งสุดท้าย

จากนั้น xR = xR XOR P17 และ xL = xL XOR P18 ในที่สุดให้รวมเข้าด้วยกันอีก xL และ xR เพื่อรับค่าที่ได้การถอดรหัสนั้นเหมือนกับการเข้ารหัสยกเว้นว่าจะใช้ P-array P1, P2, ... , P18 ในลำดับย้อนกลับดังที่แสดงในรูปที่ 1

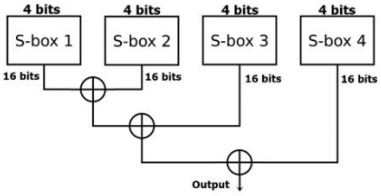


รูปที่ 1 ขั้นตอนวิธีการเข้ารหัสและถอดรหัสโบลว์ฟิช

2.2 สร้างคีย์ย่อย

เริ่มต้น P-array ก่อนแล้วตามด้วยคีย์ย่อยในเอสบล็อกสี่บล็อกตามลำดับ แต่นี้ประกอบด้วยตัวเลขฐานสิบหกของค่าพาย(น้อยกว่า 3 เริ่มต้น): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344 ฯลฯ XOR P1 ที่มี 16 บิตแรกของคีย์ XOR P2 ที่มี 16 บิตที่สองของคีย์และอื่น ๆ สำหรับบิตทั้งหมดของคีย์ (อาจสูงถึง P17) วนซ้ำรอบคีย์บิต ทั้งหมดถูก XOR ด้วยบิตคีย์

กระบวนการสร้างคีย์ย่อยได้รับการออกแบบมาเพื่อรักษาเอนโทรปีทั้งหมดของคีย์และแจกจ่ายเอนโทรปีนั้นอย่างสม่ำเสมอตลอดทั้งคีย์ย่อย มันถูกออกแบบมาเพื่อแจกจ่ายชุดของคีย์ย่อยที่อนุญาตแบบสุ่มทั่วทั้งโดเมนของคีย์ย่อยที่เป็นไปได้ ตัวเลขของค่าพายถูกเลือกเป็นคีย์ย่อยเริ่มต้นด้วยเหตุผล2ประการ 1.เนื่องจากเป็นลำดับแบบสุ่มที่ไม่เกี่ยวข้องกับอัลกอริทึม 2.เนื่องจากสามารถเก็บไว้เป็นส่วนหนึ่งของอัลกอริทึมหรือเมื่อจำเป็น แต่ถ้าเริ่มต้นไม่ใช่แบบสุ่มในทางใดทางหนึ่งการไม่สุ่มอัลกอริทึมในขั้นตอนนั้นหรือมีการเปลี่ยนแปลงบางคีย์ดังที่แสดงในรูปที่ 2



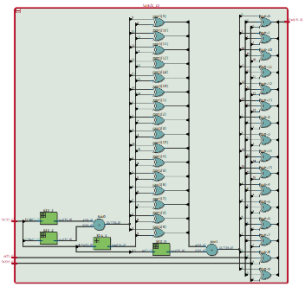
รูปที่ 2 การทำงานของฟังก์ชันบล็อก

3. การออกแบบและผลการทดลอง

3.1 ออกแบบวงจร

การออกแบบวงจรโดย Verilog HDL ด้วยโปรแกรม Altera Quartus II ซึ่งมีการเขียนโปรแกรมสร้างวงจร encyp และ decyp เป็นวงจรหลักที่มีค่า P เป็น Key หลัก และมีวงจร funS เป็นวงจรย่อยอยู่ภายใน ซึ่งภายใน วงจร funS ประกอบด้วยวงจรย่อย S3, S2, S1, S0 ซึ่งมีค่า Key ย่อยที่แตกต่างกัน

วงจรเข้ารหัส เริ่มโดยมีข้อมูลขาเข้าขนาด 32 บิตและจะถูกแยกออกเป็น xl และ xr ซึ่งมีขนาน 16 บิต ถัดไป xl ทำการ xor กับค่า P00 แล้วให้ xl เป็นข้อมูลขาออกในส่วนถัดไปให้ xr เป็นข้อมูลขาเข้าของ tin1 และ xl เป็นข้อมูลขาเข้าของ tin2 และ P01 เป็นข้อมูลขาเข้าของ pi และ xr เป็นข้อมูลขาออกของวงจร funS ดังแสดงในรูปที่ 3



รูปที่ 3 วงจรย่อย funS

ถัดไปให้ xl เป็นข้อมูลขาเข้าของ tin1 และ xr เป็นข้อมูลขาเข้าของ tin2 และให้ค่า P02 เป็นข้อมูลขาเข้าของ pi และ xl เป็นของมูลขาออกของวงจร funS ขั้นถัดสลับให้ xr และ xl เป็นข้อมูลขาเข้าของ tin1 จนถึง P16 แล้วนำ xr ทำการ xor กับ P17 แล้วสลับค่าให้ xl เป็น xr และ xr เป็น xl

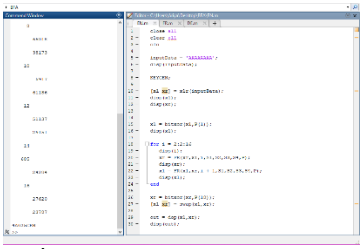
```
sum1 = sout3 + sout2
sxor1 = sum1 ^ sout1
sum2 = sxor1 + sout0
sxor2 = fin2 ^ sum2
fout = sxor2 ^ pi
```

หลักการทำงานของ funS จะทำการแบ่ง tin2 เป็นข้อมูลขาเข้า S3, S2, S1, S0 ขนาด 4 บิตหลักการทำงานของวงจรย่อย S3, S2, S1, S0 มีข้อมูลขาเข้าขนาด 4 บิตเพื่อระบุค่า Key ย่อยที่แตกต่างกันเป็นข้อมูลขาออกขนาด 16 บิต

วงจรถอดรหัส หลักการออกแบบเป็นเช่นเดียวกับวงจรเข้ารหัสแตกต่าวเพียงค่า Key หลักที่เรียงลำดับย้อนกับ

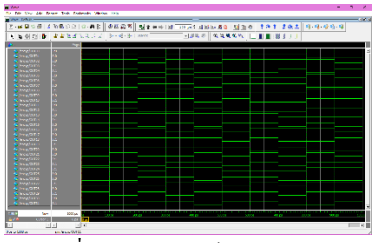
3.2 ผลการทดลอง

การทดสอบด้วยโปรแกรม Matlab โดยการกำหนดข้อมูลสำหรับเข้ารหัสและถอดรหัส ดังที่แสดงในรูปที่ 4



รูปที่ 4 การทดสอบด้วยโปรแกรม Matlab

สำหรับการทดสอบด้วยโปรแกรม Modelsim ทำโดยการป้อนข้อมูลขาเข้าขนาด 32 บิตแล้วทำการทดสอบ ดังที่แสดงในรูปที่ 5



รูปที่ 5 การทดสอบด้วย Modelsim

ผลการทดสอบการเข้ารหัสและถอดรหัสด้วยโปรแกรม Matlab และ Modelsim ดังแสดงในตารางที่ 1

ตารางที่ 1 ผลการทดสอบเข้ารหัสและถอดรหัส

ข้อมูล(ฐาน 16)	เข้ารหัส(ฐาน 16)	ถอดรหัส(ฐาน 16)
00000000	919f4003	00000000
11112222	6192662d	11112222
356abc	333eed26	356abc
aaaaaaaa	4a025ceb	aaaaaaaa
bbbbbbbb	665a23fe	bbbbbbbb

4. สรุป

ผลจากการทดสอบวงจรเข้ารหัสด้วยอัลกอริทึมโบลว์ฟิชด้วยการจำลองการทำงานด้วยโปรแกรม Modelsim ผลจากการทดสอบที่ได้เป็นข้อมูลฐาน 2 เมื่อทำการแปลงข้อมูลเป็นฐาน 16 พบว่าค่าที่ได้จากการเข้ารหัสและถอดรหัสมีความถูกต้องตามที่ได้จากการทดสอบด้วยโปรแกรม Matlab ดังนั้นสรุปได้ว่าวรจรเข้ารหัสและถอดรหัสสามารถนำไปประยุกต์ใช้งานเพื่อให้เกิดประโยชน์ตามที่ได้เสนอไว้ข้างต้น

เอกสารอ้างอิง

[1] Saneeth Kumar Chinta. (2015). Blowfish. สืบค้นเมื่อ 22 ตุลาคม 2561.การใช้งาน MATLAB เบื้องต้น.
สืบค้นเมื่อ 26 ตุลาคม 2561. จากเว็บไซต์:http://www.mathworks.com.

[2] Michael D. Ciletti. (2002). Advanced Digital Design with the Verilog HDL. University of Colorado at Colorado Springs.

ประวัติผู้เขียน

ชื่อ-สกุล	นาย คุณากร ดิษฐโรจน์
วัน/เดือน/ปีเกิด	5 มีนาคม 2540
ที่อยู่ปัจจุบัน	25/1 หมู่8 ต.ทับกวาง อ.แก่งคอย จ.สระบุรี 18260
เบอร์โทรศัพท์	098-5577157
ประวัติการศึกษา	มัธยมศึกษาตอนต้น (ม.ต้น) โรงเรียนเทศบาลบ้านม่วง พ.ศ.2552-2555 มัธยมศึกษาตอนปลาย (ม.ปลาย) โรงเรียนแก่งคอย พ.ศ. 2555-2558 ระดับปริญญาตรี (ป.ตรี) มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร พ.ศ. 2558-2562

ชื่อ-สกุล	นาย อริยะ ลักษณะสุต
วัน/เดือน/ปีเกิด	10 กันยายน 2538
ที่อยู่ปัจจุบัน	354/197 ซ.เขมาเนรมิต ถ. ประชาราษฎร์สาย 1 แขวง บางซื่อ เขต บางซื่อ กทม. 10800
เบอร์โทรศัพท์	083-2532632
ประวัติการศึกษา	มัธยมศึกษาตอนต้น (ม.ต้น) โรงเรียนสอาดเผดิมวิทยา พ.ศ. 2551-2554 มัธยมศึกษาตอนปลาย (ม.ปลาย) โรงเรียนสอาดเผดิมวิทยา พ.ศ. 2554-2557 ระดับปริญญาตรี (ป.ตรี) มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร พ.ศ. 2557-2560