BİL264 Mantıksal Devre Tasarımı
Proje Raporu
MAD Apricots

1.Giriş

Bu projede Gelişmiş Şifreleme Standardı'nda (-ing. Advanced Encryption Standard, AES) 128-bitlik veriyi yine 128-bitlik anahtar(-ing. key) kullanarak şifreleyen algoritma Verilog donanım dilinde yazdık ve test ettik. Bu algoritma 10 kere tekrar eden girdi açık metni, çıktı şifreli metne dönüştüren şifreleme çevirimlerinden(-ing. round) oluşmaktadır. Son çevirim hariç her çevirim dört adımdan oluşmaktadır. Çevrimin içindeki adımlar hakkında detaylı bilgi proje tasarımı bölümünde verilecektir.

2.Proje Tasarımı

Proje 3 temel modülden ve bu temel modüller içerisinde kullanılan yan modüllerden oluşmaktadır. Bu temel modüller, ana modül, şifreleme modülü ve anahtar modülüdür. Yan modüllerimiz ise projemizde sıklıkla kullanılan fonksiyon benzeri modüllerdir. (Ör: Bit Değişikliği, Sütun Karıştırma vb.) Tasarlamış olduğumuz bütün temel ve yan modülleri ana modülde bir araya getirilerek sade ve anlaşılır bir ana modül elde edilmiştir. Ana modülümüz ilk 9 çevrim boyunca Anahtar ve Şifreleme modülü aracılığıyla işlemlerini gerçekleştirmiştir. Ancak 10. ve son adımımız farklı bir adım olduğu için (Sütun karıştırma içermiyor.) önceden oluşturduğumuz yan modüller kullanılarak "Sifreleme_Modulu_Son" adını verdiğimiz bir modül oluşturduk ve bu modülü de ana modülümüz de kullandık. Böylece yapmaya karar vermiş olduğumuz fonksiyonvari yan modüllerimizin projemizi ne kadar adaptif hale getirdiğini görmüş olduk. Ayrıca bu modülün çıkışlarını ne zaman kullanacağımıza dair bilgiyi de hangi adımda olduğumuzu kontrol eden bir "sayac" değişkeni ile elde ediyoruz.

3. Karşılaşılan Zorluklar ve Bulunan Çözümler

3.1 Karşılaşılan Zorluklar

1.) Galois Çarpım: Galois çarpımı Sütun Karıştırma yan modülünde kullanmak durumunda olduğumuz bir işlemdi ve ilk başlarda anlamakta sıkıntı çektik.

2.) Simülasyon Sonlandırma: Simülasyonumuzu 2 değerle denemeye karar verdik ve testbench kodumuzu buna göre yazdık ancak simülasyonumuz 2. ve son değerimiz olan girdiyi sürekli giriş olarak aldı ve çıktı oluşturmaya devam etti.

3.) Modüler Olmayan Temel Modüller: Temel modüllerimizi oluşturmaya ilk başladığımız da yan modül oluşturmamıştık bundan dolayı yazmaya çalıştığımız kodlar değiştirmeye uygun olmayan anlaşılması zor kodlar haline geldi.

4.) Yavaş Şifreleme: Tasarımımızın ilk halinde 20 çevrim sonunda ilk çıkışı elde ediyorduk.

3.2) Bulunan Çözümler:

1.) Galois Çarpım: Yaptığımız araştırmalar sonucunda bulduğumuz kaynaklar genelde projemizden alakasız ve aklımızdaki soru işaretlerini silmekten uzaktı ama en sonunda hem konumuzla alakalı hem de açıklayıcı bir kaynak bulabildik. (Xintong) Bu kaynaktan yararlanarak Galois çarpımı kısmını Verilog'a uyarladık.

2.) Simülasyon Sonlandırma: Kısa bir araştırma sonucunda bu problemden kurtulmak adına işimize yarayan iki tane fonksiyon bulduk.("$finish" ve "$stop") (Renerta) Bu fonksiyonları testbenchte kullanarak bu sorunu da çözdük.

3.) Modüler Olmayan Temel Modüller: Yukarıda bahsettiğimiz üzere temel modüllerdeki karmaşıklığı engellemek adına fonksiyonvari yan modüller oluşturmaya karar verdik ve böylelikle anlaşılır ve adaptif temel modüller elde etmiş olduk.

4.) Yavaş Şifreleme: Kodumuzu daha hızlı çalıştırmak için yeni kontrol mekanizmaları ekledik. Bu sayede artık 10 çevrimde çıkış elde ediyoruz.

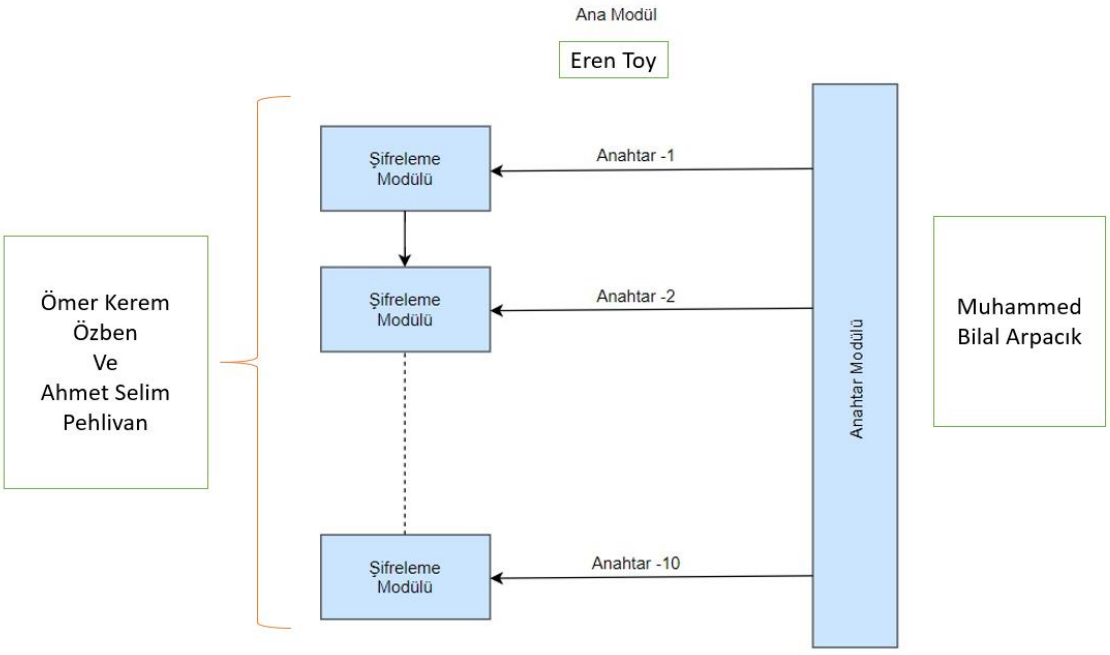
4. Gerçekleştirilemeyenler

Proje ön raporunda belirttiğimiz ve gerçekleştiremediğimiz herhangi bir durumla karşılaşmadık.

5. İş Bölümü:

Bu projeyi gerçeklerken 4 üye de kendi başlarına araştırma yapmış daha sonrasında elde edilen veriler ışığında proje planlaması yapılmış ve yol haritası çıkarılmıştır.

Ömer Kerem Özben ve Ahmet Selim Pehlivan şifreleme modülünü, Eren Toy ana modülü, Muhammed Bilal Arpacık anahtar modülünü tasarlamak üzere görevlendirilmiştir. Bu görev bölümü Diyagram 5.1'de gösterilmiştir.



Diyagram 5.1: *Modüller Arası İletişim*

Kaynakça

Renerta . (tarih yok). *Simulation Control Tasks.* Renerta : https://verilog.renerta.com/mobile/source/vrg00042.htm adresinden alındı

Xintong, K. C. (tarih yok). *Understanding AES Mix-Columns Transformation Calculation.* http://www.angelfire.com/biz7/atleast/mix_columns.pdf adresinden alındı