Mantıksal Devre Tasarımı Proje Raporu

1.Giriş

Bu projede uluslararası alanda defacto şifreleme standardı olarak kullanılan AES 128 şifreleme sistemi Verilog ile tasarlanmıştır.

2. Proje Planlaması

AES (Advanced Encryption Standart) simetrik bir şifreleme dilidir. Simetrik algoritmalarda tek bir gizli anahtar bulunur, şifreleme ve şifre çözme için bu anahtara ihtiyaç duyulur. AES algoritmasında girdi ve çıktı matrisleri 128 bitliktir. Bu matris 4 satır ve 4 sütundan oluşur(4x4) ve bu matrise "durum" adı verilmektedir.

S0	S4	S8	S12
S1	S5	S9	S13
S2	S6	S10	S14
S3	S7	S11	S15

Şekil 1.1 Örnek Durum Matrisi

AES algoritması 128 bitlik veri bloklarının şifrelenmesini sağlamaktadır. AES algoritması işlemlerini bu matris üzerinde gerçekleştirdiğinden, şifrelenecek veri uygun bir şekilde durum matrisi halinde ifade edilmelidir.

Oluşturulan bu durum matrisi her bir turda bazı işlemlerden geçer:
1. Bayt değiştirme
2. Satır Kaydırma
3. Sütun Karıştırma
4. Tur Anahtarı ile Toplama

Sütun karıştırma işlemi son turda uygulanmaz.

AES algoritması 128 bit veri bloklarını 128, 192 veya 256 bit anahtar seçenekleri ile şifreler. AES şifrelemesi anahtar uzunluğuna göre farklı sayıda döngü içerir.

AES-128 için tur sayısı: 10
AES-192 için tur sayısı: 12
AES-256 için tur sayısı: 14

Verilog’da AES 128’i gerçeklemek için başta giriş olarak, 128’er bitlik bir anahtar bir de şifrelenmek istenen metin alınır. AES 128’de şifreleme işlemini gerçekleştirmek için prosedürün 10 tur uygulanması gerektiği belirtilmişti. 10 tur uygulama aşamasında, her turun bitişi bir clock sinyali sayesinde anlaşılır ve bir sonraki tura geçiş yapılır.

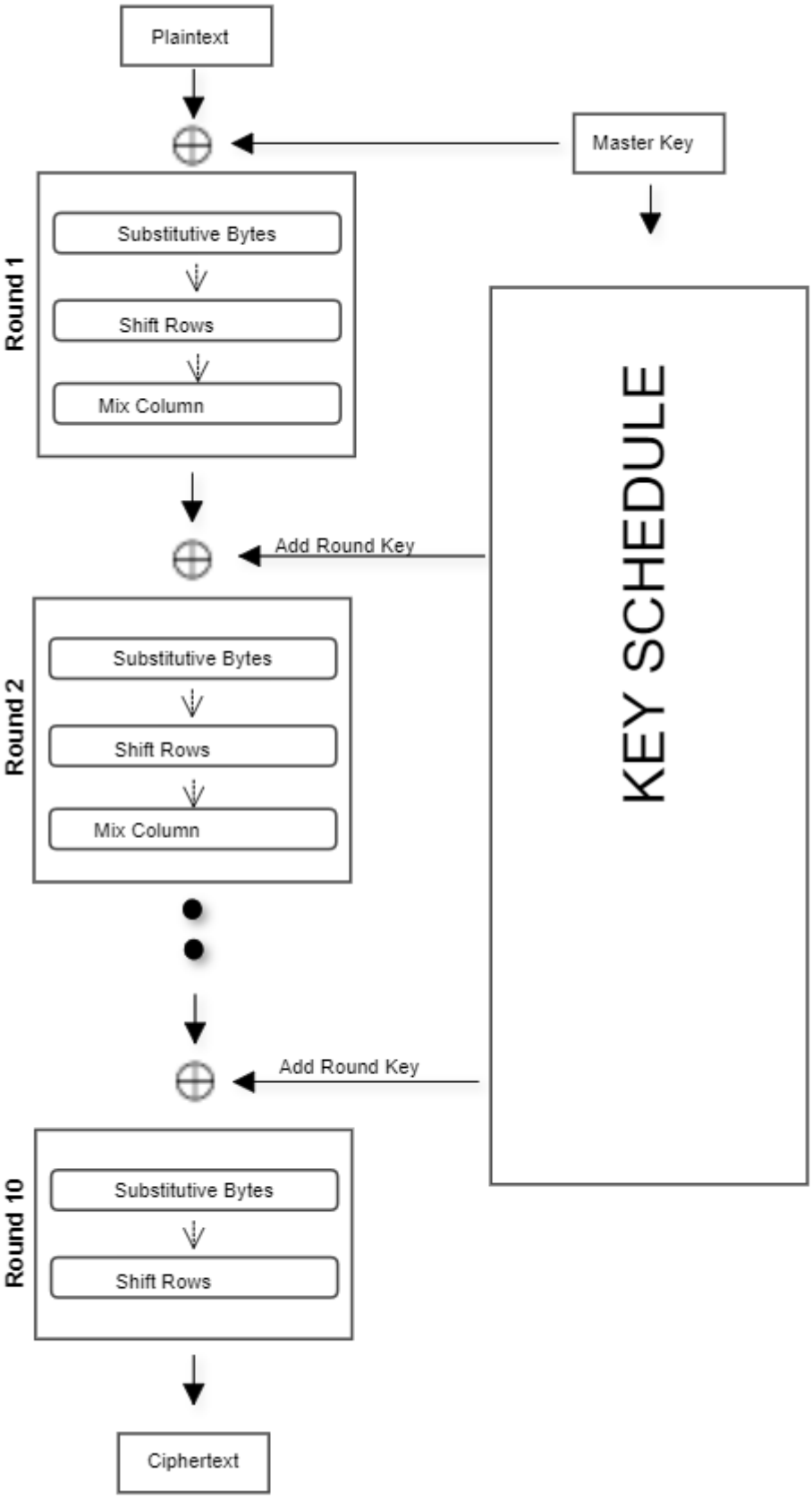
Bu kriptografi sisteminde ayrı ayrı modüller oluşturulup bir ana modül üzerinde birleştirilmesi amaçlanmaktadır. Modüller birbiri ile alışveriş halinde olup birinin çıktısı, diğerinin girdisi olacak şekilde bir akış sağlanır.

Verilog Projesi’nin ana modülünde giriş olarak clk, rst, anahtar, blok, geçerlilik sinyali gibi sinyaller alınır. İlk aşamada alınan şifrelenecek metin blok[127:0], durum matrisine dönüştürülür ve oluşturulan bu durum matrisi ana anahtar ile XOR işlemine tabi tutulur.

Ardından XOR işlemine tabi tutulan durum matrisi Bayt Değiştirme aşamasında S-Box’taki değerler ile değiştirilir. Burada değişime uğrayan durum matrisi bir sonraki aşama olan Satır Kaydırma modülüne ilerler.

Satır kaydırma işlemi tamamlandıktan sonra formu değişen durum matrisi, sütun karıştırma işlemine ilerler. Bu aşamada durum matrisi A matrisi ile çarpma işlemine tabi tutulur ve sütun karıştırma işlemi gerçekleşir.

Turun son aşamasında şifrelenmiş hale gelen durum matrisi bir kez de tur anahtarı ile XOR işlemine tabi tutulur ve gerçekleşecek 10 turdan ilki tamamlanmış olur. Bu aşamalar 10 kez gerçekleştiğinde şifreleme işlemi tamamlanır ve şifrelenmiş durum matrisi çıktı olarak verilir.


Plaintext
Master Key
Round 1
Substitutive Bytes
Shift Rows
Mix Column
KEY SCHEDULE
Add Round Key
Round 2
Substitutive Bytes
Shift Rows
Mix Column
Add Round Key
Round 10
Substitutive Bytes
Shift Rows
Ciphertext

2.1 Bayt Değiştirme (SubBytes)

Bayt Değiştirme aşaması anahtar eklendikten sonra olan çevrimlerin ilk aşamasıdır ve algoritmanın doğrusal olmayan tek adımıdır. Bu aşamada durum matrisinde bulunan her baytın değeri bir tablo doğrultusunda ve lineer olmayan bir şekilde güncellenir. Bu aşama girdileri baytlara ayırıp hepsini bir değişim kutusundan geçirmeyi içerir. AES Şifrelemede DES şifrelemenin aksine her bayt için aynı değişim kutusu kullanılır.

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

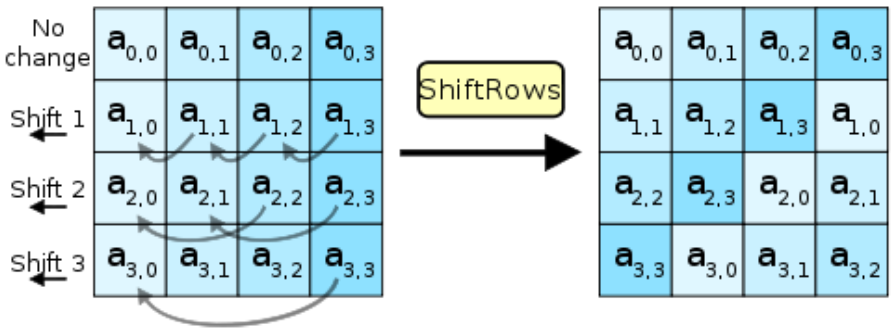
[1] Şekil 2.1 AES S-Box

Bayt Değiştirme adımında, 8 bitlik bir değişim kutusu (substitution box, Fotoğraf 1.1) kullanılarak yapılan güncelleme sayesinde algoritmanın doğrusallığı bozulur ve non-linear formuna ulaşması sağlanır. S-Box yüksek doğrusal-olmayanlık (nonlinearity) özelliğine sahip sonlu cisim üzerinde ters alma işleminden elde edilmiştir. Bu da algoritmanın doğrusallığını bozmasının asıl sebebidir.

Daha iyi anlaşılması açısından, bir bölmedeki değerin S0 = {57} olsun. Dikey olarak 5, yatay olarak da 7 bulunduğunda S'0 = {5b} değerine ulaşılır. Bayt değiştirme aşamasının temel mantığı bu şekildedir. Bayt Değiştirme işlemi sonucunda ulaşılan matris, satır kaydır işlemine gönderilerek işleme devam edilir.

2.2 Satır Kaydır (ShiftRows)

Satır Kaydır adımı İsminden de anlaşıldığı üzere doğrudan satır kaydırma işlemi yapılır. Bayt değiştirme sonucu üretilen matrisin her satırının bayt değerlerini belirli sayıda kaydırma işleminin uygulandığı adımdır. İlk satır değiştirilmez iken diğer satırlar sırası ile 1, 2 ve 3 bayt sola kaydırılır. Yani ikinci satır 1 bayt kaydırılarak 2. Satırdaki bütün elemanlar bir sonraki sütuna geçer, en son sütundaki eleman da ilk sütunda boş kalan yere yazılır. 3. ve 4. satırda da bir fazlası bayt kaydırma yapılarak aynı işlemler tekrarlanır.



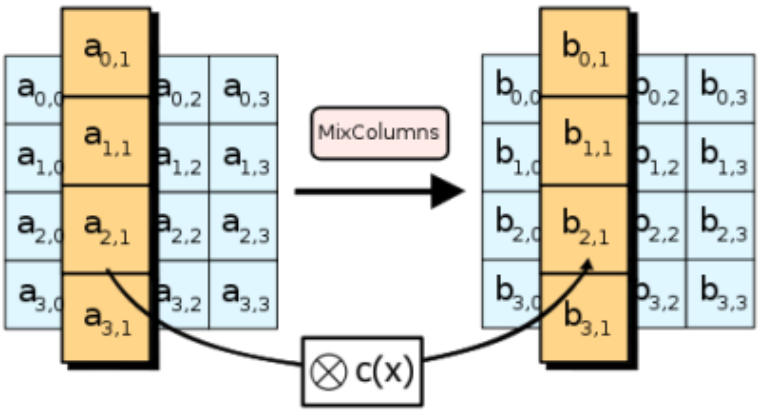
[2] Şekil 3.1 Kaydırma Öncesi ve Sonrası Matris

2.3 Sütun Karıştırma (MixColumns)

Projemizin sütun karıştırma bölümünde diğer aşamalara kıyasla daha basit bir işlem yapıyoruz. Bu aşamada, bir önceki aşamadan çıktı olarak gelen kaydırılmış matrisin her sütununu belirli bir A matrisi ile çarpıyoruz. Bu çarpım sonucu elemanların yerleri değişerek karılmış oluyor. Bu işlemi Verilog dilinde kodlamak kapı düzeyinde oldukça zor. Ancak burada imdadımıza davranışsal modelleme yetişiyor. Verilogda davranışsal modelleme kullanmak kodlama sürecini oldukça kısaltıyor ve bir o kadar da kolaylaştırıyor. Davranışsal modelleme sayesinde matris çarpımını kodlamak oldukça basit hale geliyor. Bahsi geçen A matrisi Şekil 4.1'de gösterilmiştir.

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Şekil 4.1 A Matrisi



[3] Şekil 4.2 Sütun Karıştırma İşlemi

2.4 Anahtar Ekleme (AddRoundKey)

Anahtar ekleme katmanında her bir turun güncel durum verisi ile tur anahtarı arasında basit bir XOR işlemi yapılır. Her bir turda anahtar belli bir algoritmaya göre değişir.

Anahtar Üretimi (KeySchedule)

AES şifrelemede her döngüde farklı bir anahtarın girişi sağlanır. Bu anahtarların üretimi kullanıcı tanımlı ana anahtarın (Master Key) anahtar üretimi fonksiyonuna sokulmasıyla gerçekleşir ve bütün anahtarlar bir önceki turda üretilen anahtarın kullanılmasıyla elde edilir. Üretilen anahtarlar sırasıyla round fonksiyonuna dahil olurlar. İlk turun anahtarı kullanıcı tarafından tanımlanmış olması gerekir. İlk üretilmiş anahtar ikinci turda fonksiyona dahil olur.

Tur sayısına N matris boyutunu 4xK olarak kabul edersek, daha sonra yapılacak işlemlerle genişlemiş matrisin boyutu 4x(Kx(N+1)) olur.

Anahtar bitlerinden oluşan matristeki son sütunun (M4) ilk elemanının sona kaydırılmasıyla başka bir sütun oluşturulur ve S-Box kullanılarak bayt değiştirme işlemi uygulanır.

M4{K1, K2, K3, K4} = M4{K2, K3, K4, K1} = S-Box ({K2, K3, K4, K1})

Bu elde edilen sütun ile ilk sütun(M1) ve önceden tanımlanmış Rcon (Round constant) vektör matrisinin 1. sütununu arasında XOR işlemi yapılır. Bu işlem sonucu oluşan yeni sütun matrise 5. sütun olarak eklenir ve yeni üretilen anahtarımızın ilk sütunu olur.

M5 = M1{K1, K2, K3, K4} $\oplus$ S-Box ({K2, K3, K4, K1}) $\oplus$ {Rcon,00,00,00}

Rcon vektörünün hangi sütununun ekleneceği hangi turda olduğuna göre değişiklik gösterir.

$$rcon_i = \begin{bmatrix} rc_i & 00_{16} & 00_{16} & 00_{16} \end{bmatrix}$$

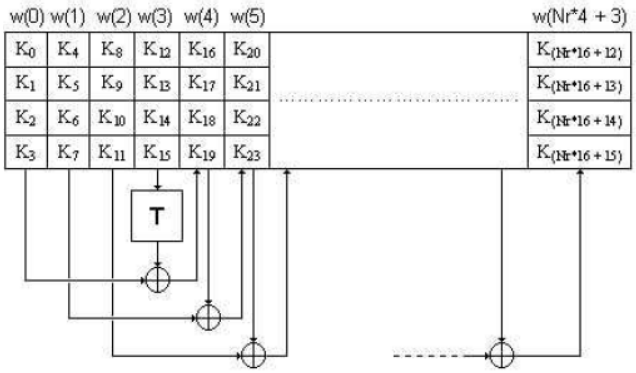
$$rc_i = \begin{cases} 1 & \text{if } i = 1 \\ 2 \cdot rc_{i-1} & \text{if } i > 1 \text{ and } rc_{i-1} < 80_{16} \\ (2 \cdot rc_{i-1}) \oplus 11\text{B}_{16} & \text{if } i > 1 \text{ and } rc_{i-1} \geq 80_{16} \end{cases}$$

i	1	2	3	4	5	6	7	8	9	10
rci	01	02	04	08	10	20	40	80	1B	36

Daha sonra bu elde edilen sütun ile 2. sütun arasında XOR işlemi yapılır ve bu yeni sütun matrise 6. sütun olarak eklenir.

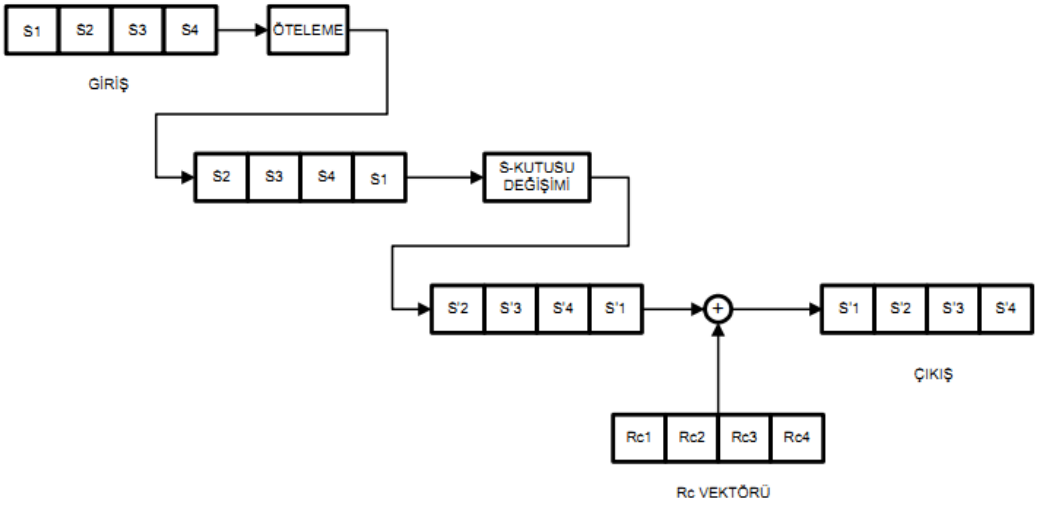
M6 = M5{A1, A2, A3, A4} $\oplus$ M2{K1, K2, K3, K4}

Matrisin K katı olan sütuna gelindiğinde 5. sütun üretilirken yapılan işlemler tekrarlanır. Bu işlemler tur sayısı kadar devam eder.



Şekil 5.1 Anahtar Üretimi Şeması

Şekilde 128 bitlik bir anahtar bloğu gösterilmektedir. Anahtar üretimi işleminde oluşan yeni matrisin ilk sütunu hesaplanırken "T işlemi" olarak gösterilen blok ile ayrı bir işlem uygulanır. Bu işlem, öteleme, S-Box kullanılarak bayt değiştirme ve Rcon vektörü ile toplama işlemlerinden oluşan bir zinciri içermektedir. Diğer sütunlar hesaplanırken o sütundan bir önceki ve dört önceki sütunlar arasında XOR işlemi yapılır.



Şekil 5.2 Anahtar Üretimi Şeması II

Kaynakça

https://en.wikipedia.org/wiki/AES_key_schedule (23.06.2020)

https://cryptography.fandom.com/wiki/Rijndael_key_schedule (19.06.2020)

https://www.comparitech.com/blog/information-security/what-is-aes-encryption/ (20.06.2020)

http://bilgisayarkavramlari.sadievrenseker.com/2009/06/03/aes-ve-rijndeal-sifreleme/ (20.06.2020)

https://medium.com/@yavuzunver/aes-ile-veri-%C5%9Fifreleme-daef840f10f3 (23.06.2020)

https://web.itu.edu.tr/~orssi/thesis/2017/BurakAcar_bit.pdf (17.06.2020)

[1,2] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#The_ShiftRows_ste (23.06.2020)

https://www.comparitech.com/blog/information-security/what-is-aes-encryption/ (21.06.2020)

https://tr.wikipedia.org/wiki/AES (23.06.2020)

https://stackoverflow.com/questions/13392365/how-to-declare-a-2d-array-in-verilog-i-want-to-take-a-4x4-matrix-as-an-input (10.06.2020)

https://github.com/secworks/aes (10.06.2020)

http://cryptographicprocessor.weebly.com/uploads/2/4/5/3/24530999/aes.pdf (20.06.2020)

https://www.comparitech.com/blog/information-security/what-is-aes-encryption/ (10.06.2020)

https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5 (23.06.2020)

http://bilgisayarkavramlari.sadievrenseker.com/2009/06/03/aes-ve-rijndeal-sifreleme/ (23.06.2020)