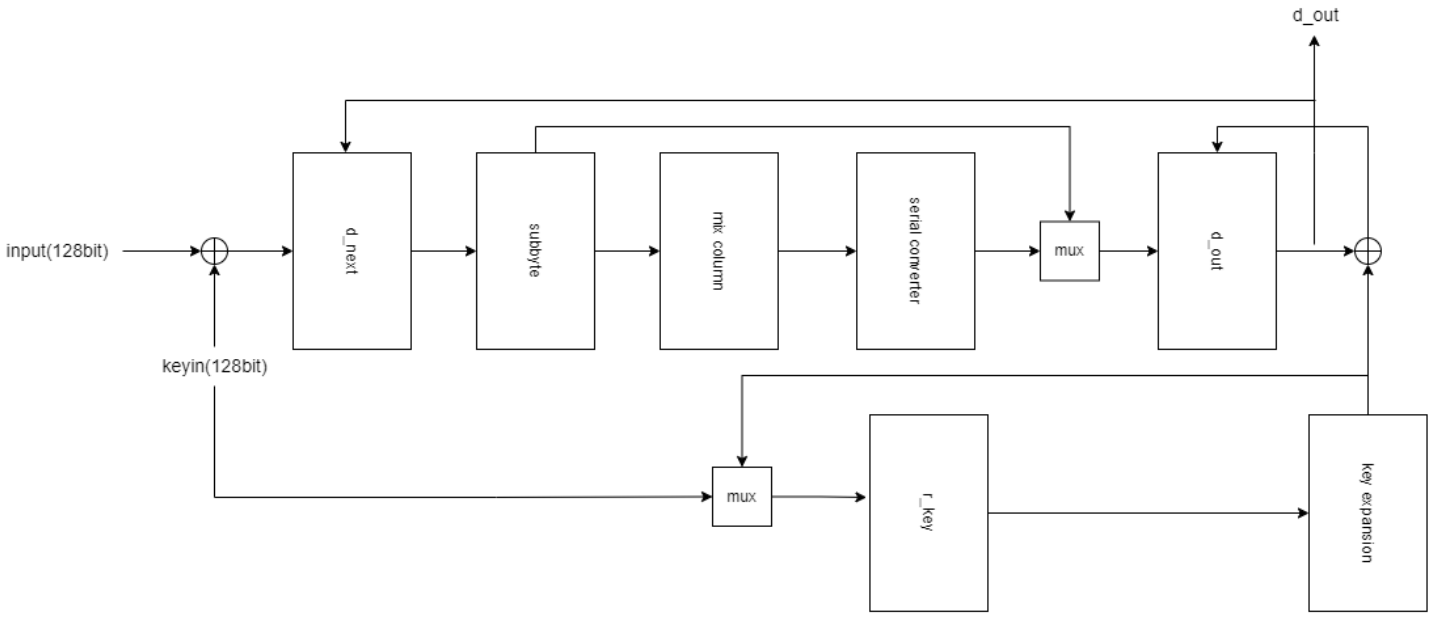
هما بدیعی 9912762278

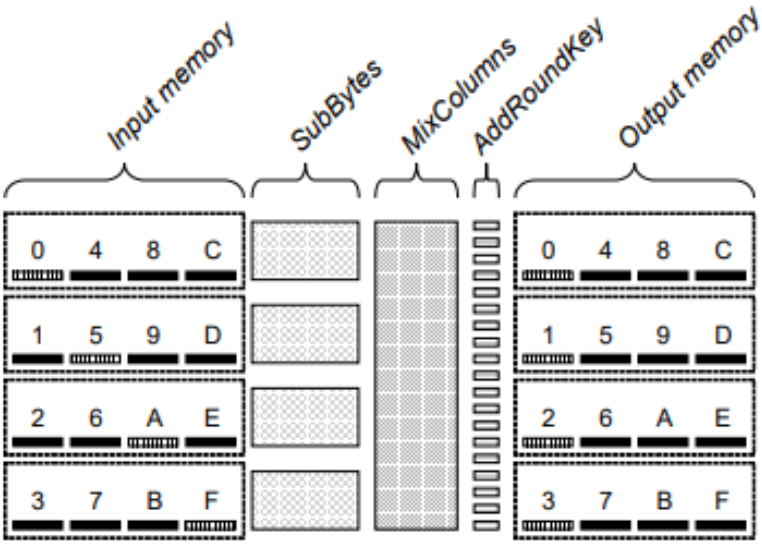
گزارش پروژه AES

در معماری زیر، ورودی های $input$ و $keyin$ 128 بیتی می باشند. رجیستر d_out , d_next 128 بیتی می باشند. الگوریتم شامل 10 راند است که در راند اولیه تنها ورودی های $input$ و $keyin$ باهم xor می شوند و در d_next به عنوان ورودی راند دوم قرار می گیرد. در 9 راند بعدی عملیات $shiftrows$ و $subbytes$ و $mix\ columns$ و $Add\ Round\ Key$ انجام می شود که در این معماری ، داده ها به صورت 8 بیتی های با ترتیب خاص ($shiftrows$) انتخاب شده و به ماژول $Sbox$ فرستاده می شوند سپس خروجی این ماژول به ماژول $mix\ columns$ فرستاده می شود. خروجی این ماژول 32 بیتی است و پس از 4 کلاک نتیجه صحیح را بر روی خروجی قرار می گیرد. خروجی این ماژول به ماژول $serial\ converter$ فرستاده می شود تا خروجی 32 بیتی به صورت 8 بیتی در دسترس قرار بگیرد و در d_out نوشته شود. در مرحله آخر از این راند، d_out با کلید همان راند که توسط ماژول $key\ expansion$ تولید می شود، xor می شود و در d_out ذخیره می شود سپس در ابتدای راند بعد مقدار d_out در d_next قرار می گیرد تا به عنوان داده ورودی برای راند بعد مورد استفاده قرار بگیرد. در راند آخر نیز تمامی این مراحل انجام می شوند اما مرحله $mix\ columns$ انجام نمی شود و خروجی $Sbox$ مستقیما در d_out قرار می گیرد.



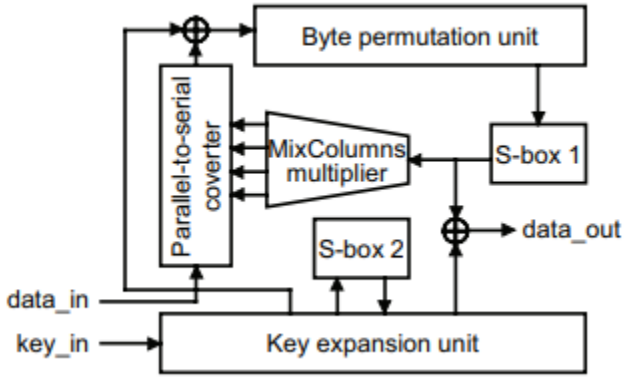
تصویر1- معماری AES

نحوه خواندن و نوشتن بایت ها در رجیسترهای d_next و d_out از شکل زیر ایده گرفته شده است (مقاله



تصویر2- نمایش نحوه خواندن بایت ها از ورودی و نوشتن آن ها در خروجی

مربوطه در پیوست قرار دارد) و معماری کلی نیز از شکل زیر ایده گرفته شده است (مقاله مربوطه در پیوست



تصویر3- نمایش معماری کلی مشابه

قرار دارد) تعداد منابع مصرفی در فایل aes_util.rpt به طور کامل قابل مشاهده هستند. جدول زیر بخشی از آن است که تعداد فلیپ فلاپ های لازم، اسلایس ها و جداول جستجو را نمایش می دهد.

Site Type	Used	Fixed	Available	Util%
Slice LUTs*	912	0	3750	24.32
LUT as Logic	912	0	3750	24.32
LUT as Memory	0	0	2400	0.00
Slice Registers	495	0	7500	6.60
Register as Flip Flop	495	0	7500	6.60
Register as Latch	0	0	7500	0.00
F7 Muxes	64	0	4000	1.60
F8 Muxes	32	0	2000	1.60

تصویر4- نمایش تعداد منابع مصرفی

اطلاعات مربوط به کلاک (از جمله فرکانس مدار) در جدول زیر قابل مشاهده است.

Clock Summary

Clock	Waveform(ns)	Period(ns)	Frequency(MHz)
clk	{0.000 50.000}	100.000	10.000

تصویر5- نمایش خلاصه اطلاعات کلاک

مطابق اطلاعات جدول زیر فرکانس کاری مدار می تواند به $F = \frac{1}{2.15} = 465MH$ افزایش بیابد.

Pulse Width Checks

Clock Name: clk
Waveform(ns): { 0.000 50.000 }
Period(ns): 100.000
Sources: { clk }

Check Type	Corner	Lib Pin	Reference Pin	Required(ns)	Actual(ns)	Slack(ns)	Location	Pin
Min Period	n/a	BUFG/I	n/a	2.155	100.000	97.845		clk_IBUF_BUFG_inst/I
Low Pulse Width	Slow	FDRE/C	n/a	0.500	50.000	49.500		d_next_reg[50]/C
High Pulse Width	Fast	FDRE/C	n/a	0.500	50.000	49.500		d_next_reg[50]/C

تصویر6- نمایش اطلاعات بررسی $pulse\ width$

پس از 215 کلاک نتیجه حاصل می شود.