تاریخ دریافت:۱۳۹۴/۰۱/۲۰
تاریخ پذیرش:۱۳۹۴/۰۵/۰۵

فصلنامه علوم و فنون نظامی/ سال دهم/ شماره ۲۹/ پائیز ۱۳۹۳
صص ۱۳۹-۱۵۸

طراحی بهینه ماژول کلید رمز AES برای ارتباطات رادیویی بلادرنگ

حسن رفیعی یکتا[۱]
جلیل مظلوم[۲]
احمد زوار تربتی[۳]

چکیده

با گسترش ارتباطات رادیویی، امنیت اطلاعات در معرض تهدید قرار گرفت. رمزکننده‌ها برای کاهش خطرات ناشی از استفاده نادرست از ارتباطات رادیویی بکار گرفته‌شدند. البته رمزکننده‌هایی که سابقاً در این حوزه مورد استفاده قرار می‌گرفتند بسیار ضعیف بودند و به راحتی شکسته می‌شدند. یکی از الگوریتم‌های رمز که اخیراً در سامانه‌های ارتباط رادیویی مورد استفاده قرار می‌گیرد، الگوریتم رمز AES است. البته استفاده از این الگوریتم در ارتباطات رادیویی به تازگی متداول شده است و سابقه طولانی ندارد. در این مقاله روش پیاده‌سازی معماری تکراری الگوریتم AES مورد بررسی قرار می‌گیرد و یک روش جدید برای اجرای کدر و دیکدر الگوریتمAES بر روی سخت‌افزار واحدFPGA پیشنهاد می‌گردد. برای بررسی نتایج پیاده‌سازی هر دو روش، از سه نوع سخت‌افزار مختلفFPGA در دو حالت بهینه شده برای سرعت و حجم استفاده شده است. نتیجه پیاده سازی الگوریتم رمز AES به روش پیشنهادی، افزایش گذردهی، صرفه جویی در سخت‌افزار و انرژی مورد نیاز است.

واژگان کلیدی:

استاندارد رمزنگاری AES ، سخت افزار FPGA، گیرنده و فرستنده رادیوییRTX ، زبان توصیف سخت افزار VHDL.

---

[۱] - مربی دانشکده مهندسی برق، دانشگاه علوم و فنون فارابی
[۲] - استادیار دانشکده مهندسی برق، دانشگاه علوم و فنون هوایی شهید ستاری
[۳] - دانشجوی دکتری مهندسی برق – مخابرات (سیستم) دانشگاه صنعتی مالک اشتر

مقدمه

رمزنگاری در لغت به معنای تغییر داده به اطلاعات محرمانه با همان طول اولیه است. رمزنگاری علاوه بر استفاده در سامانه‌های اقتصادی، سیاسی و نظامی در سامانه‌های رادیویی کاربرد فراوانی دارد. رمزنگاری سامانه‌های ارتباط رادیویی مانع دسترسی راحت سامانه‌های شنود بیگانه به اطلاعات محرمانه می‌گردد. البته لازم به ذکر است که قرار دادن رمز در سیگنال‌های رادیویی به معنای امنیت مطلق برای این سیگنال‌ها نیست؛ بلکه فقط سطح دسترسی را کاهش می‌دهد در صورتی که شخص تحلیل‌گر اراده کند می‌تواند با بررسی ترافیک ارتباطات رادیویی، توان فرستنده‌ها، زمان و مکان ارسال پیام، طول زمان برقراری ارتباط و ... اطلاعات ارزنده‌ای از هدف خود بدست آورد[۱].

رمزکننده‌ای که در شبکه‌های رادیویی مورد استفاده قرار می‌گیرد باید دارای سرعت پردازش بالایی باشد تا بتواند پیام‌های رادیویی را بصورت بلادرنگ رمزگذاری و رمزگشایی نماید. بدلیل محدویت ابعاد و اندازه رادیوهای متحرک اندازه و ابعاد رمزکننده‌های رادیویی بایستی تاحد ممکن کوچک باشد. همچنین محدودیت دیگر رمزکننده‌های مورد استفاده در سامانه‌های رادیویی محدودیت در منابع انرژی موجود در رادیوهای متحرک است. بنابراین پارامترهایی مانند سرعت پردازش، ابعاد و اندازه رمزکننده، و انرژی مورد نیاز آن در استفاده از رمزکننده در سامانه‌های رادیویی محدودیت بوجود می‌آورد. در انتخاب یک رمزکننده برای ارتباط رادیویی سرعت پردازش آن از اهمیت بالایی برخوردار است؛ به‌طور قطع یقین کاربران ارتباطات رادیویی تأخیر در ارسال و دریافت پیام را نمی‌پذیرند.

شبکه‌های ارتباط رادیویی

غالب شبکه‌های رادیویی اعم از آنالوگ یا دیجیتال در ۲ نوع زیر طراحی و اجرا می‌شوند.

۱- شبکه‌های رادیویی کانال مستقیم[۲] (Direct Channel)

در این نوع شبکه ارسال و دریافت پیام، در یک کانال، با استفاده از یک فرکانس رادیویی انجام می‌شود. مزیت اصلی آن برقراری سریع آن با کمترین تعداد فرکانس و کانال است. مشکل اصلی این نوع شبکه ناحیه کم پوشش رادیویی آن است.

۱- روشی که در حال حاضر در سامانه‌های جنگ الکترونیک کاربرد دارد این است که می‌توان با استفاده از سامانه DF(Direction Finder) محل دقیق ارسال سیگنال رادیویی، توان رادیویی فرستنده و کلی اطلاعات ارزنده دیگر را بدست آورد و با تحلیل اطلاعات با ارزش بدست آمده توان رزمی دشمن را تحلیل کرد.

۲- ساده‌ترین نوع شبکه رادیویی است که در آن فرکانس ارسال و دریافت رادیوها باهم برابر است.

۲- شبکه‌های رادیویی کانال غیرمستقیم[۱] (Repeater channel)

برای بهره‌وری هر چه بیشتر شبکه‌های رادیویی، طراحی به گونه‌ای انجام می‌شود که ناحیه پوشش شبکه تا حد مورد نیاز گسترش یابد؛ به این منظور از تکرارکننده‌های رادیویی در شبکه‌ها استفاده می‌شود. تکرارکننده‌های رادیویی عمل تقویت سیگنال را در شبکه انجام می‌دهند.

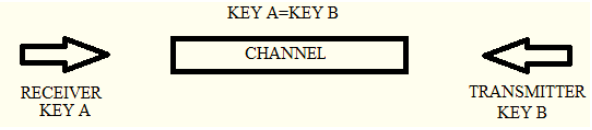
کلیات رمزنگاری

اصلی‌ترین بحثی که در این مقاله به آن پرداخته می‌شود طراحی بهینه ماژول کلید رمز AES[۲] است؛ به همین خاطر در مورد الگوریتم‌های رمزنگاری توضیح مختصری داده می‌شود.

۱- الگوریتم رمزنگاری کلید خصوصی یا کلید متقارن

در این الگوریتم (تنها نوع رمزنگاری تا قبل از دهه ۷۰)، فقط از یک کلید برای رمز و کشف رمز استفاده می‌شود؛ به همین خاطر به آن رمزنگاری کلید متقارن یا " تک کلیدی " هم گفته می‌شود. چالش اصلی دراین نوع الگوریتم چگونگی تبادل کلید بین دو طرف گیرنده و فرستنده پیام است. از جملهٔ الگوریتم‌های معروف در زمینهٔ رمزنگاری متقارن، الگوریتم DES[۳] است. با توجه به ظهور پردازنده‌های قوی، که توانایی تحلیل و شکستن الگوریتم DES را دارند؛ بتدریج DES جای خود را به الگوریتم رمز AES داده است.، AES استاندارد جدید رمزنگاری متقارن زیر نظر NIST[۴] است. انتظار می‌رود که AES امنیت رمزنگاری قوی برای حفاظت اطلاعات حساس در قرن بیست‌ویکم فراهم کند. الگوریتم رمز AES به دلیل استحکام و انعطاف‌پذیری خوب به عنوان الگوریتم استاندارد در بین سایر الگوریتم‌های متقارن بلوکی معرفی شده است. شکل (۱) گویای نحوه استفاده از این نوع رمزکننده‌ها است. (هادی سمیعی، شهریور ۱۳۸۶)

شکل ۱) رمزنگاری با کلید خصوصی



---

[۱]- در این نوع شبکه رادیوها بطور غیر مستقیم و با استفاده از یک واسط رادیویی به‌نام تکرارکننده کار می‌کنند؛ فرکانس ارسال و دریافت رادیوها باهم متفاوت است؛ و یک فاصله چند مگاهرتزی باهم دارند.

2 . Advanced Encryption Standard

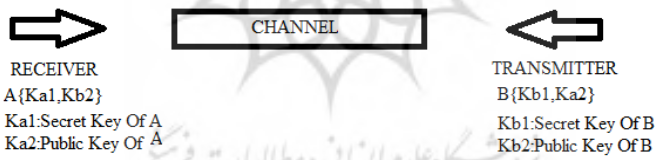
3 . Data Encryption Standard

4 . National Institute Of Standards And Technology

۲- الگوریتم رمزنگاری کلید عمومی یا کلید نامتقارن

این الگوریتم که برای حل مشکل انتقال کلید در الگوریتم کلید متقارن ابداع گردید؛ برای رمزنگاری از دو کلید مختلف یعنی کلید عمومی[1] و کلید خصوصی[2] استفاده می‌کند؛ یعنی هر کدام از طرفین فرستنده و گیرنده یک جفت کلید دارند. روال انجام کار به این ترتیب است که ابتدا فرستنده با استفاده از کلید عمومیِ گیرنده، پیام را رمزگذاری می‌کند و گیرنده پیام را با کلید خصوصی خودش رمزگشایی می‌کند. پس بدون آنکه فرستنده و گیرنده، کلیدی را به اشتراک بگذارند، می‌توانند پیام‌هایشان را بصورت امن مبادله کنند. در این نوع رمزنگاری، کلیدهای رمزگذار[3] و رمزگشا[4] متمایز از هم هستند و یا این‌که چنان رابطه پیچیده‌ای بین آن‌ها حاکم است که کشف کلید دیکدر با در اختیار داشتن کلید کدر، عملاً ناممکن است. الگوریتم رمزنگاری کلید عمومی ذاتاً کندتر از الگوریتم رمزنگاری کلید خصوصی است. از الگوریتم‌های نامتقارن می‌توان RSA، ElGamal، Diffie-Hellman را نام برد. شکل (۲) گویای نحوه استفاده از این نوع رمزکننده‌ها است (کیوان منصوری، شهریور ۱۳۸۸)

شکل ۲)رمزنگاری با کلید عمومی



مبانی نظری تحقیق:

پیشرفت‌های اخیر در سامانه‌های ارتباط رادیویی باعث گسترش روزافزون شبکه‌ها و کانال‌های رادیویی گردیده است. درعین‌حال، قابلیت اطمینان به شبکه‌های ارتباط رادیویی نیز افزایش پیداکرده است. همین امر باعث رشد کاربران شبکه‌های رادیویی شده است. علت و محرک اصلی گسترش این نوع شبکه‌ها قابلیت حمل، تحرک، و در دسترس بودن این نوع شبکه‌ها است. اگرچه مخابرات باسیم ثبات بیشتر، عملکرد بهتر، و قابلیت اطمینان بالاتری دارد اما محدود به مکان خاص است (جعفرخانی،۲۰۰۵). در حالی که این مشکل در

1. Public Key
2. Secret Key
3. Coder
4. Decoder

ارتباطات رادیویی وجود ندارد. مشکل اساسی ارتباطات رادیویی در امنیت شکننده آن است. الگوریتم رمز AES به تازگی در شبکه‌های رادیویی مورد استفاده قرار می‌گیرد[۱]. در اکثر موارد، طراحان رمزکننده‌ها از دو برد کُدر و دیکُدر به‌عنوان ماژول رمز استفاده می‌کنند[۲]؛ این نوع طراحی باعث افزایش تأخیر در ارسال و دریافت اطلاعات می‌گردد. در کاربردهای غیرهمزمانِ ارتباط بین گیرنده و فرستنده پیام، این نوع طراحی قابل قبول است و هیچ مشکلی در آن مشاهده نمی‌شود ولی در کاربردهایی با سرعت بالا مانند ارتباط همزمان بین گیرنده و فرستنده این نوع طراحی کارایی چندانی ندارد.

ریاضیات پایه الگوریتم رمز AES

در الگوریتم AES چندین عملیات مختلف ریاضی در سطح بایت انجام می‌شود با توجه به این‌که هر یک از بایت‌های مورد استفاده، عنصری از میدان متناهی $GF(2^8)$ است؛ در این بخش به معرفی مفاهیم پایه ریاضیات مورد نیاز می‌پردازیم. مقدار یک بایت در $GF(2^8)$ به‌عنوان مجموعه‌ای از بیت‌های ۰ و ۱ نمایش داده می‌شود اشکال مختلف توصیف عناصر میدان گالوسی $GF(2^8)$ همگی باهم معادل هستند همه عملیات انجام‌شده در AES بر مبنای مدول ۲ است. (J.Org J. Buchholz, December, 2001:19)

$$B_7 X^7 + B_6 X^6 + B_5 X^5 + B_4 X^4 + B_3 X^3 + B_2 X^2 + B_1 X + B_0 \quad -(۱$$

عملیات جمع در الگوریتم رمز AES

این عملیات در توصیف چندجمله‌ای بین تک‌تک عناصر دو ورودی با ضرایب توان‌های یکسان و به پیمانه عدد ثابت ۲ صورت می‌گیرد. این عملیات همان XOR منطقی است.

عملیات ضرب در الگوریتم رمز AES

ضرب با نماد ۰ نمایش داده می‌شود. حاصل‌ضرب مدولار دو چندجمله‌ای در حوزه میدان متناهی $GF(2^8)$ بر یک چندجمله‌ای ساده نشدنی از درجه ۸ تقسیم می‌شود. این چندجمله‌ای ساده نشدنی برای الگوریتم AES عبارت زیر است:

$$M(X) = X^8 + X^4 + X^3 + X + 1 \quad (۲)$$

---

[۱]– به عنوان نمونه شرکت Hytera که در زمینه تولید تجهیزات رادیویی فعالیت می‌کند؛ از الگوریتم رمز AES بعنوان رمزکننده در تجهیزات رادیویی استفاده کرده است.

[۲]– در اکثر تکرارکننده‌های رادیویی از دو برد مجزا برای رمز و کشف رمز پیام استفاده می‌شود.

عملیات ضرب چندجمله‌ای با x (مقدار ثابت ۲)

چندجمله‌ای‌های چهارجمله‌ای، چندجمله‌ای‌های هستند که تعداد آن‌ها ۴ جمله است و ضرایب آن‌ها عضو میدان متناهی گالوسی هستند مانند:

$$A(X)=A_3X^3+A_2X^2+A_1X+A_0 \qquad (۳)$$

در اینجا $A_3A_2A_1A_0$ تشکیل یک کلمه را می‌دهند. حاصل‌ضرب چندجمله‌ای B(X) در X به‌صورت زیر نمایش داده می‌شود:

$$P(X) = B(X)*X = B_7 X^8 +B_6 X^7 +B_5 X^6 +B_4 X^5 +B_3 X^4 +B_2 X^3 +B_1 X^2 +B_0 X \qquad (۴)$$

و جواب نهایی رابطه بالا با محاسبه چندجمله‌ای P(X) به پیمانه M(X) حاصل خواهد شد. اگر در چندجمله‌ای P(X) بیت B_7 برابر صفر باشد آنگاه اعمال پیمانه M(X) به P(X) معادل خود P(X) هست و فقط زمانی که B_7 برابر با یک باشد، اعمال پیمانه M(X) معادل با تفاضل این چندجمله‌ای از چندجمله‌ای P(X) هست. با توجه به موارد مطرح‌شده واضح است که ضرب یک چندجمله‌ای در سطح بایت با X (معادل عددی ۲H)، معادل شیفت بیتی آن به سمت چپ به میزان‌یک واحد و پس از آن XOR نمودن شرطی حاصل با عدد "1B"H هست. شرط ذکرشده با توجه به مقدار بیت B_7 تعیین می‌شود؛ این عملیات را که با Xtime(A) نمایش می‌دهند. در برخی از سخت‌افزارهای خاص با ۴ عملگر XOR قابل پیاده‌سازی هست. (Samiee, Hadi, 2010 IEEE)

معکوس چند جمله‌ای در میدان متناهی $GF(2^8)$

برای یافتن معکوس چندجمله‌ای B(X) در میدان متناهی $GF(2^8)$ از الگوریتم توسعه‌یافته می‌توان استفاده نمود. طبق این الگوریتم رابطه زیر همیشه برقرار هست:

$$B(X).\ A(X) + M(X).\ C(X) = 1 \qquad -(۵)$$

که در آن C(X) یک چندجمله‌ای دلخواه و M(X) یک چندجمله‌ای تحویل‌ناپذیر در میدان متناهی GF(28) هست.

الگوریتم کُدر و دیکُدر AES

الگوریتم کدر و دیکدر AES مبتنی بر الگوریتم رایندال[1] هست این الگوریتم روی‌داده‌هاو کلیدهای به‌طول ۱۲۸، ۱۹۲ و ۲۵۶ بیتی کار می‌کند، که در این‌جا فقط بر روی کلید و داده متن ۱۲۸ بیتی بحث می‌شود. برای شروع به کار کُدر و دیکُدر ابتدا بایستی کلید و متن ورودی در ماتریس حالت و ماتریس کلید قرار گیرند. آرایه‌های ماتریس حالت و

[1] -Rijndeal(Daemen, J. and Rijmen) رایندال مخفف نام دو محققی است که این الگوریتم را طراحی کرده‌اند

ماتریس کلید ۸ بیتی هستند بنابراین برای AES/128 تعداد ۱۶ آرایه در یک ماتریس ۴*۴ قرار می‌گیرند. الگوریتم رمز AES از چهار تبدیل مبتنی بر بایت (بایت گرا) تشکیل‌شده است این تبدیلات شامل تبدیلات زیر است.(Rajender Manteena, March 23, 2004)

جانشینی بایت[1]

این تبدیل یک عملیات جانشینی بایتی غیرخطی هست و بر روی هر یک ازبایت‌های ماتریس حالت به‌صورت مستقل انجام می‌شود. این تبدیل خود از ترکیب دو زیر تبدیل حاصل‌شده است که عبارت‌اند از:

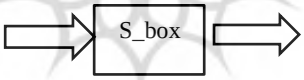
الف)- محاسبه وارون ضربی ورودی در میدان متناهی GF(28).

ب)- اعمال تبدیل آفینی به خروجی حاصل از مرحله قبل.

بکارگیری کلیه مراحل فوق بر روی تمام بایت‌های ماتریس حالت با جانشینی بایت نمایش داده می‌شود و به‌طور خلاصه به آن S_Box گویند. درشکل (۳) چگونگی اثر این تبدیل بر روی ماتریس حالت ورودی ارائه شده است. (Pallavi Atha, Suresh, Gyan,Vihar,May 2010)

شکل ۳) نمایش جایگزینی با جدول S-BOX

$A_{0,0}$	$A_{0,1}$	$A_{1,2}$	$A_{0,3}$
$A_{1,0}$	$A_{1,1}$	$A_{1,2}$	$A_{1,3}$
$A_{2,0}$	$A_{2,1}$	$A_{1,2}$	$A_{2,3}$
$A_{3,0}$	$A_{3,1}$	$A_{3,2}$	$A_{3,3}$



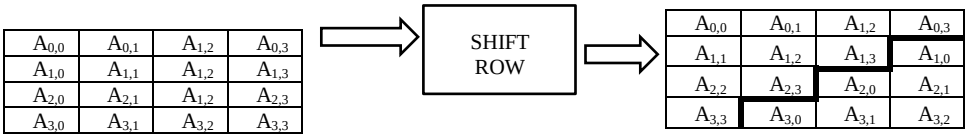
$B_{0,0}$	$B_{0,1}$	$B_{1,2}$	$B_{0,3}$
$B_{1,0}$	$B_{1,1}$	$B_{1,2}$	$B_{1,3}$
$B_{2,0}$	$B_{2,1}$	$B_{1,2}$	$B_{2,3}$
$B_{3,0}$	$B_{3,1}$	$B_{3,2}$	$B_{3,3}$

شیفت سطری[2]

در این تبدیل به هر یک از ردیف‌های ماتریس حالت ورودی، به‌اندازه معینی شیفت چرخشی اعمال می‌شود. اثر اعمال این نوع تبدیل بر روی ماتریس حالت ورودی در شکل (۴) آورده شده است.

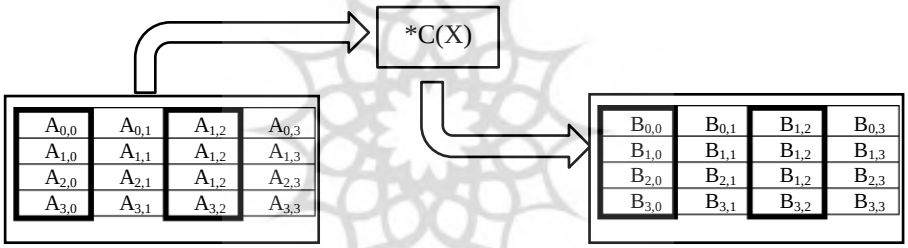
1.Sub Byte
2.Shift Row

شکل ۴) اثر تبدیل شیفت سطری بر روی ماتریس حالت



ترکیب ستونی[1]

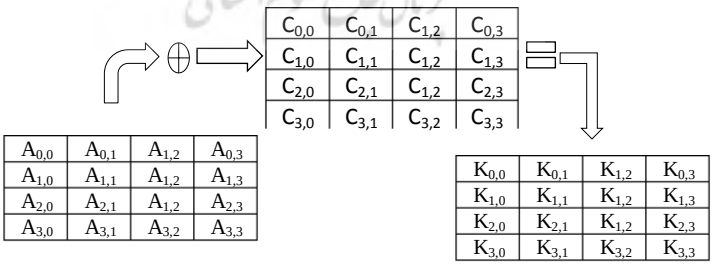
در این تبدیل هر یک از ستون‌های ماتریس حالت ورودی به‌عنوان یک چندجمله‌ای بر روی میدان متناهی GF(28)در نظر گرفته می‌شود. حاصل‌ضرب این چندجمله‌ای با چندجمله‌ای ثابت C(X) و شیفت‌های متوالی آن به پیمانه X4+1 محاسبه گشته و خروجی را نتیجه می‌دهد. در شکل (۵) نحوه اثر تبدیل ترکیب ستونی بر روی ماتریس حالت نشان داده شده است.



جمع‌کردن با کلید دور[2]

در این تبدیل زیر کلید مربوط به هر مرحله با ماتریس حالت مربوط XOR می‌گردد. در شکل (۶) جمع‌کردن با کلید دور و ماتریس حالت نشان داده شده است.

شکل ۶) اثر جمع کلید رمز با ماتریس حالت

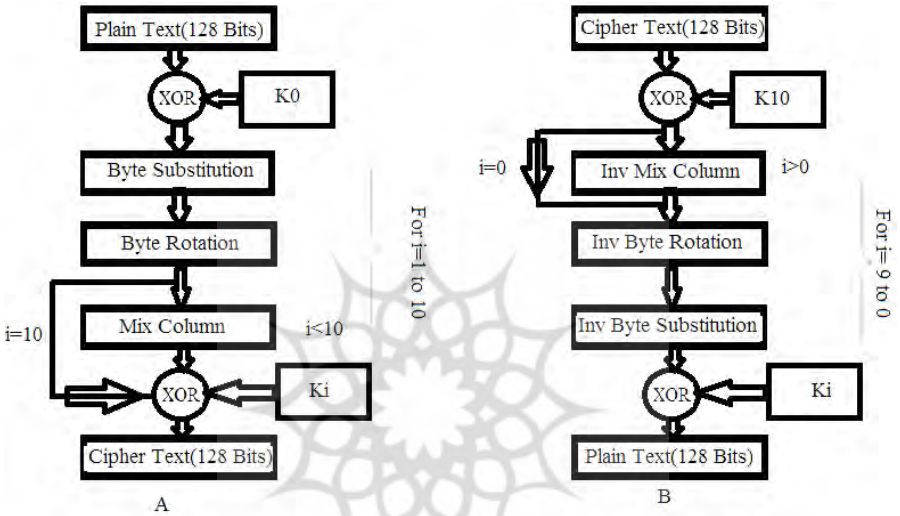


1. Mix Column
2 .Add Round Key

واحد تولید و بسط کلید

وظیفه واحد بسط کلید، تولید کلید برای هرکدام از دورها با استفاده از کلید اصلی است؛ کلید اصلی از کاربر گرفته می‌شود. واحد بسط کلید جمعاً تعداد ۴۴ کلید ۳۲ بیتی برای AES/128 تولید می‌کند. الگوریتم اجرای کدر و دیکدر AES در شکل (۷) نشان داده شده است.

شکل۷) الگوریتم اجرای AES شکل A کُدر و شکل B دیکُدر



برای پیاده‌سازی رمز AES معماری‌های مختلفی وجود دارد که در این‌جا فقط معماری تکراری به اختصار توضیح داده می‌شود.

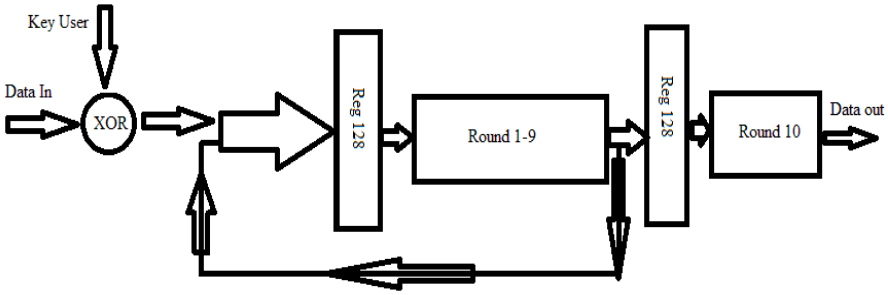
۱) معماری AES تکراری[1]

دو روش مبتنی بر تکرار برای الگوریتم رمز AES وجود دارد. روش اول که به آن معماری تکراری پایه‌ای گفته می‌شود برای رمزنگاری داده‌ها فقط از یک مجموعه سخت‌افزار استفاده می‌کند. این روش تعداد واحدهای CLB[2] کمتری از FPGA اشغال می‌کند اما سرعت آن نسبت به نوع دوم کمتر است و درنتیجه گذردهی[3] آن پایین‌تر است در روش دوم برای اجرای دور ۱ الی ۹ از یک مجموعه سخت‌افزار و برای دور دهم از یک مجموعه سخت‌افزار دیگر استفاده گردیده است (توجه داشته باشید که در الگوریتم رمز AES دور آخر کدر و

1.Iterative
2. Configurable Logic Block
3. Throughput

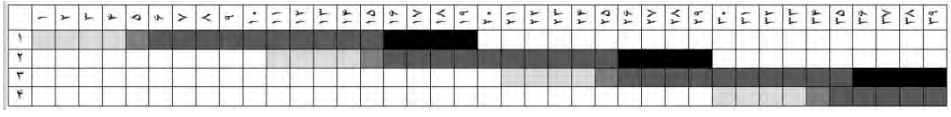
دیکدر نسبت به سایر دورها اندکی متفاوت است). این روش به‌جای ۱۰ سیکل از ۹ سیکل استفاده می‌کند درنتیجه گذردهی آن بالاتر از قبلی است ولی حجم سخت‌افزار آن نیز بالاتر است شکل (۸) اشاره به روش نوع دوم دارد. (کیوان منصوری، شهریور ۱۳۸۸)

شکل ۸) معماری تکراری با از استفاده ۹ سیکل



برای جمع‌آوری دیتای مورد نیازِ بلوک بسط کلید و همچنین متن اصلی[1] برای بلوک ورودی، و متن رمزشده[2] در بلوک خروجی دو روش جمع‌آوری ۸ بیتی و جمع‌آوری ۳۲ بیتی وجود دارد. این دو روش در تمامی معماری‌های AES کاربرد دارد. در تمامی معماری‌ها هر یک از دورهای الگوریتم رمز AES یک سیکل به طول می‌انجامد (مستقل از نوع معماری)، بنابراین در معماری AES تکراری پایه‌ای (روش اول) رمزگذاری بسته اول ۱۱ سیکل طول می‌کشد (یک سیکل برای عملیات XOR اولیه) چهار سیکل نیز برای جمع‌آوری داده‌ها اختصاص می‌یابد، بنابراین تأخیر اولیه مدار ۱۵ سیکل می‌شود. بعد از تأخیر اولیه داده‌های رمز شده بعد از هر ۱۰ سیکل آماده برداشت می‌شود؛ زیرا عملیات XOR بسته دوم همراه دور آخر بسته اول انجام می‌شود. همچنین در هنگام انجام دور پنجم الگوریتم توسط بلوک داده، بلوک ورودی شروع به جمع‌آوری بسته داده جدید می‌کند (صرفه‌جویی در مصرف کلاک). زمان‌بندی اعمال این کلاک بر عهده واحد کنترل است. جزئیات کامل معماری تکراری پایه‌ای AES، دیاگرام زمانی ماشین حالت[3] آن به ترتیب در جدول ۱ و ۳ و شکل (۹) ارائه‌شده است. (منصوری، ۱۳۸۸)

جدول ۱) دیاگرام زمانی معماری تکراری الگوریتم AES

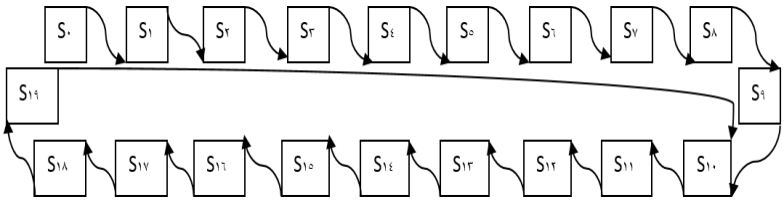


1. Plain Text
2. Cipher Text
3. State Machine

جدول ۲) راهنمای جدول ۱

بلوک ورودی		xor		بلوک داده		بلوک خروجی	

شکل ۹) دیاگرام حالت برای معماری تکراری پایه‌ای



جدول ۳) سیگنال‌های کنترلی معماری AES تکراری پایه‌ای کُدر

state	خروجی‌های ماشین حالت
S0	مرحله RESET
S1	010_0000(32bit MSB d127-d96)
S2	001_0000(32bit MSB d95-d64)
S3	000_1000(32bit MSB d63-d32)
S4	000_0100(32bit MSB d31-d0)
S5	100_0000(xor)
S6	000_0000 دور اول
S7	000_0000 دور دوم
S8	000_0000 دور سوم
S9	000_0000 دور چهارم
S10	000_0000 دور پنجم
S11	010_0000 دور ششم(32bit MSB d127-d96)
S12	001_0000 دور هفتم(32bit MSB d95-d64)
S13	000_1000 دور هشتم(32bit MSB d63-d32)
S14	000_0100 دور نهم(32bit MSB d31-d0)
S15	100_0010 دور دهم(xor)
S16	010_0000 دور اول(32bit MSB O127-O96)
S17	000_0001 دور دوم(32bit MSB O95-O64)
S18	000_0001 دور سوم(32bit MSB O63-O32)
S19	000_0001 دور چهارم(32bit MSB O31-O0))

بهره‌وری هر مداری بر اساس نسبت بین به‌کارگیری قطعات سخت‌افزار (تعداد واحدهای CLB اشغال‌شده) و گذردهی آن تعریف می‌شود. در FPGA به‌کارگیری قطعات به معنی تعداد واحدهای CLB اشغال‌شده توسط مدار است. گذردهی هر مدار مشخص‌کننده تعداد

بیت‌های رمز شده در ثانیه به‌وسیله مدار است. فرض کنید فرکانسی که مدار با آن کار می‌کند 'X' هرتز باشد و 'Y' تعداد سیکل‌های لازم برای رمزگذاری 'Z' بیت داده باشد در این صورت گذردهی واحد کدر به‌صورت زیر تعریف می‌شود:.(Samiee, Hadi, 2010 IEEE)

$$T= (X/Y)*Z\ Bp \quad (۶)$$

معماری‌هایی که برای افزایش گذردهی طراحی گردیدند، در حقیقت متغیر Y (مخرج کسر) را اصلاح کردند. برای معماری تکراری پایه‌ای که تماماً مبتنی بر تکرار است، متغیر Y=10 خواهد بود. در معماری‌هایی مانند معماری خط‌لوله یک مرحله‌ای[1] و خط‌لوله چهارمرحله‌ای[2] این متغیر به ترتیب به ۵ و ۲ کاهش پیدا خواهد کرد که منجر به افزایش گذردهی خواهد شد. (با توجه به رابطه گذردهی معماری‌ها تفاوت آن‌چنانی در فرکانس باهم ندارند.) جدول (۴) و جدول (۵) ماکزیمم فرکانس عملی، گذردهی و فضای اشغال‌شده توسط طرح معماری تکراری پایه‌ای را نشان می‌دهد. این بررسی‌ها روی چندین سخت‌افزار FPGA شرکت زایلینکس[3] انجام‌شده است.

جدول ۴) نتایج سنتز معماری تکراری پایه‌ای کدر در چندین قطعه FPGA بهینه‌شده[4] برای سرعت[5]

سخت‌افزار	SLICE	FLIP-FLOP	LUTS	FREQUENCY (Mhz)	گذردهی (گیگابایت بر ثانیه)
XC3S1000-5FG320	۱۵۰۰	۱۴۵۲	۲۴۰۳	۱۴۸.۰۷۴۱	۱.۸۹۵۳۴۸۴۸
Xc4vfx12-12SF363	۱۵۱۹	۱۴۴۵	۲۳۶۳	۲۳۲.۵۸۰	۲.۹۷۷۰۲۴
XC7285TL-1LFFG1157	۱۴۳۳	۱۲۶۸	۹۱۳	۵۳۱۸۰۹	۶.۸۰۷۱۵۵۲

جدول ۵) نتایج سنتز معماری تکراری پایه‌ای کدر در چندین قطعه FPGA بهینه‌شده برای حجم[6]

سخت‌افزار	SLICE	FLIP-FLOP	LUTS	FREQUENCY (Mhz)	گذردهی (گیگا بیت بر ثانیه)
XC3S1000-5FG320	۱۲۹۹	۱۳۱۰	۲۱۸۲	۱۳۰.۸۷۹	۱.۶۷۵۲۵۱۲
Xc4vfx12-12SF363	۱۳۳۱	۱۳۱۰	۲۱۸۲	۲۲۸.۳۳۲	۲.۹۲۲۶۴۹۶
XC7285TL-1LFFG1157	۱۲۹۷	۱۲۵۲	۱۰۱۶	۴۶۰.۳۴۲	۵.۸۹۲۳۷۷۶

1 .Pipe Line
2 .Sub Pipe Line
3. Xilinx
4. Optimized
5. Speed
1. Area

تجزیه و تحلیل

روش پیشنهادی (اجرای همزمان کدر و دیکدر)

در این روش کدر و رمزگشا هر دو بر روی یک سخت افزار پیاده سازی و به صورت همزمان کار می‌کنند. به دلیل رابطه مستقیمی که بین کلید کدر و دیکدر وجود دارد به راحتی می‌توان از یک سخت افزار برای تولید کلید مورد نیاز کّدر و دیکُدر استفاده کرد. در حالی‌که در روش‌های قبلی از دو سخت افزار جدا از هم برای تولید کلید استفاده گردیده است.

دلایل استفاده همزمان از کُدر و دیکُدر AES

تکرار کننده‌ی رادیویی از یک دستگاه گیرنده و یک دستگاه فرستنده تشکیل می‌گردد. تکرارکننده پیام رادیویی را از طریق گیرنده خود دریافت و در همان زمان بدون هیچ گونه تأخیر همان پیام را از طریق فرستنده خود ارسال می‌کند. در خیلی از موارد لازم است تغییراتی در پیامی که از گیرنده دریافت شده است بوجود آید و سپس به فرستنده ارسال گردد. به‌عنوان مثال سیگنال پیامی از طرف گیرنده دریافت شده است و حال لازم است در ماهیت سیگنال پیام تغییراتی داده شود؛ در این حالت ابتدا بایستی از پیام دریافتی کشف رمز به عمل آید و سپس تغییرات در پیام بوجود آید و دوباره پیام رمز گردیده و به سمت فرستنده ارسال شود. در صورت استفاده از روش‌های موجود در سامانه‌های ارتباط رادیویی تأخیر ارتباط بین فرستنده، و گیرنده زیاد می‌شود و برای سامانه‌های رادیویی این تأخیر مشکل ساز می‌گردد. علاوه براینکه به دلیل کمبود تجهیزات شاید لازم باشد از دستگاه تکرارکننده، علاوه بر کار تکرارکنندگی به‌عنوان رادیوی مرکزی استفاده شود. در این وضعیت یک کاربر، با در اختیار گرفتن ورودی تکرارکننده می‌تواند اقدام به ارسال پیام کند. تکرارکننده بایستی، باید بطور همزمان سیگنال دریافتی از گیرنده و سیگنال دریافتی از ورودی میکروفن را رمز نموده و ارسال نماید.

الگوریتم پیشنهادی بایستی توانایی کار در بی‌سیم‌های[1] دستی و خودرویی[2] را داشته باشد. نحوه کار رادیوهای دستی به اینصورت است که در یک لحظه، رادیو گیرنده و یا فرستنده است. وقتی‌که بی‌سیم دستی به‌عنوان فرستنده کار می‌کند اطلاعات از طریق مدار میکروفن وارد ماژول کُدر می‌شود و اطلاعات رمز شده پس از پیمودن مسیرهای مربوط، از طریق

1. Radiomoble

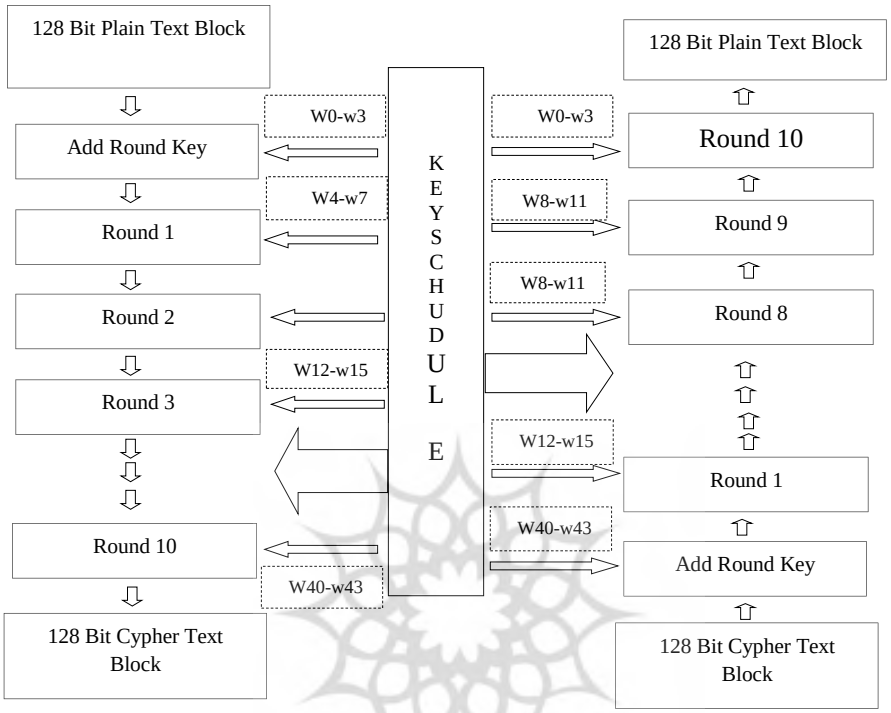
۲- بی‌سیم خودرویی نوعی رادیو است که در خودرو نصب می‌شود و توان خروجی بالاتری نسبت به بی‌سیم دستی دارد

آنتن ارسال می‌شود. زمانی‌که بی‌سیم دستی بعنوان گیرنده کار می‌کند، اطلاعات از طریق آنتن بی‌سیم وارد رادیو می‌شود؛ پس از آشکارسازی پیام وارد مدار کشف رمز می‌شود و اطلاعات اصلی از آن استخراج می‌شود. در روش پیشنهادی با یک سخت‌افزار هر دو ماژول کدر و دیکدر در یک مدار طراحی می‌شود، در این صورت نیاز به مدار کنترل برای انتخاب ماژول کدر و دیکدر نیست چون فقط یک مدار برای کدر و دیکدر وجود دارد.

پیاده سازی کُدر و دیکُدر در یک سخت‌افزار (روش پیشنهادی)

در این روش با استفاده از یک سخت افزار برای پیاده سازی هر سه ماژول کدر و دیکدر و سخت افزار توسعه کلید، گذردهی مدار بالا می‌رود. سخت افزار توسعه کلید رمز پس از دریافت کلید اصلی، اقدام به تولید ده زیرکلید دیگر می‌نماید که این ده زیرکلید در ده دور داده کاربرد دارد. در الگوریتم رمز متقارن برخلاف رمز نامتقارن کلیدِ رمز و کلید کشفِ رمز یکی است. در این حالت کلیدی که برای رمز کردن پیام کاربرد دارد دقیقاً همان کلیدی است که برای کشف رمز کاربرد دارد. اما یک تفاوت که در رمزنگاری AES وجود دارد این است که کلید اولی که درکدر به‌عنوان کلید رمز به کار می‌رود کلید آخری است که در رمزگشا برای کشف رمز کاربرد دارد. به همین ترتیب کلید دوم کدر، کلید ماقبل آخر دیکدر است. با توضیحاتی که داده شد مشخص می‌شود که می‌شود که با استفاده از یک سخت افزار می‌توان کلید مورد نیاز کدر و دیکدر را تولید کرد، فقط در طراحی مدار بایستی با ابتکار عمل، از یک برنامه برای تولید کلید استفاده نمود. شکل (۱۲) گویای استفاده از یک سخت افزار تولید کلید رمز برای تولید زیر کلیدهای مورد نیازکدر و دیکدر است. این روش برای طول کلید ۱۲۸،۱۹۲،۲۵۶ بیت نیز کاربرد دارد.

شکل ۱۲) پیاده‌سازی همزمان کدر و دیکدر در یک سخت افزار با استفاده از یک ماژول بسط و توسعه کلید



بررسی نتایج کدر و دیکدر AES در روش پیشنهادی با استفاده از نرم‌افزار ISE

به منظور آزمایش روش پیشنهادی، ابتدا به برنامه رمز گذار AES یک متن داده و یک کلید رمز ۱۲۸ بیتی اعمال می‌شود و پس از اجرای برنامه در محیط شبیه‌ساز ISE خروجی متن رمز شده بدست می‌آید[۱]. سپس طرح سنتز می‌شود و طرح در یک FPGA پیاده‌سازی می‌شود. برای پیاده‌سازی طرح‌ها از سخت‌افزارهای مختلف استفاده می‌شود. طرح ابتدا روی سخت‌افزار مجازی موجود در نرم‌افزار ISE جانمایی و مسیریابی می‌شود. عملیات یک رشته بیت تولید می‌کند. رشته بیت تولیدی، سخت‌افزار را برنامه‌ریزی می‌کند.

همانطور که قبلاً عنوان گردید در رابطه گذردهی X فرکانسی است که مدار با آن کار می‌کند و از سنتز مدار بدست می‌آید و Y تعداد سیکل‌های لازم برای اجرای کامل الگوریتم رمزنگاری است که در حالت معماری تکراری عدد ۱۰، برای حالت خط لوله یک مرحله‌ای

[۱] - لازم به ذکر است که درستی نتایج با استفاده از نرم‌افزار Matlab نیز بررسی شده است

یک مرحله ای عدد ۵ و برای خط لوله چهار مرحله‌ای عدد ۲ است. اگر برای هر کدام از ماژول‌های DEC و ENC یک ماژول تولید و بسط کلید مجزا در نظر گرفته شود در این صورت$Z=128$ و در صورتی که با روش پیشنهادی این مقاله ماژول تولید و بسط کلید طراحی گردد $Z=256$ است. در حقیقت Z تعداد بیت‌هایی است که برنامه روی آن عملیات انجام می‌دهد. نتایج جداول زیر از تحلیل سخت‌افزار توسط نرم‌افزار ISE به دست‌آمده است. سطر آخر جداول نتیجه سنتز معماری پایه‌ای به روش پیشنهادی است.

جدول ۱۱) سنتز معماری تکراری پایه‌ای با روش پیشنهادی استفاده از سخت‌افزار XC3S1000-5FG320 بهینه شده برای سرعت

ماژول	SLICE	FLIP-FLPO	LUTS	FREQUENCY (Mhz)	T(bps)
ENC	۱۵۰۰	۱۴۵۲	۲۴۰۳	۱۴۸.۰۷۴۱	۱.۸۹۵۳۴۸
DEC	۱۹۴۸	۱۷۳۷	۳۵۸۰	۱۴۷.۶۴۸	۱.۸۸۹۸۹۴
DECENC	۳۷۵۷	۴۴۰۹	۵۵۸۳	۱۰۷.۹۷۶	۲.۷۶۳۶

جدول ۱۲) سنتز معماری تکراری پایه‌ای با روش پیشنهادی سخت‌افزار از 36SF12-12VFX4XC بهینه شده برای سرعت

ماژول	SLICE	FLIP-FLPO	LUTS	FREQUENCY (Mhz)	(bps)
ENC	۱۵۱۹	۱۴۴۵	۲۳۶۳	۲۳۲.۵۸۰	۲.۹۷۷۰۲۴
DEC	۱۹۸۶	۱۷۲۸	۳۵۸۸	۲۸۷.۵۵۰	۳.۶۸۰۰۶۴
DECENC	۴۰۵۷	۴۴۰۵	۶۰۱۶	۲۲۷.۱۲۰	۵.۸۵۹۶۹۶

جدول۱۳) سنتز معماری تکراری پایه‌ای با روش پیشنهادی استفاده از سخت‌افزار XC7285TL-1LFFG1157 بهینه شده برای سرعت

ماژول	SLICE	FLIP-FLPO	LUTS	FREQUENCY (Mhz)	Z(bps)
ENC	۱۴۳۳	۱۲۶۸	۹۱۳	۵۳۱.۸۰۹	۶.۸۰۷۱۵۵۲
DEC	۱۶۸۹	۲۰۵۹	۱۱۶۹	۴۹۷.۱۱	۶.۳۶۳۰۰۸
DECENC	۴۳۷۷	۳۴۲۵	۱۹۴۲	۴۹۶.۷۳۲	۱۲.۷۱۶۳۳۹۲

جدول ۱۴) سنتز معماری تکراری پایه‌ای با روش پیشنهادی استفاده از سخت‌افزار XC3S1000-5FG320 بهینه شده برای حجم

ماژول	SLICE	FLIP-FLPO	LUTS	FREQUENCY (Mhz)	Z(bps)
ENC	۱۲۹۹	۱۳۱۰	۲۱۸۲	۱۳۰.۸۷۹	۱.۶۷۵۲۵۱۲
DEC	۱۷۸۲	۱۵۶۶	۳۲۱۶	۱۱۸.۶۸۰	۱.۵۱۹۱۰۴
DECENC	۳۲۲۳	۴۲۶۸	۵۳۷۴	۱۰۰.۶۷۴	۲.۵۷۷۲۵۴۴

جدول ۱۵) سنتز معماری تکراری پایه‌ای روش پیشنهادی استفاده از سخت‌افزار 36SF12-12VFX4XC بهینه شده برای حجم

ماژول	SLICE	FLIP-FLPO	LUTS	FREQUENCY (Mhz)	Z(bps)
ENC	۱۳۳۱	۱۳۱۰	۲۱۸۲	۲۲۸.۳۳۲	۲.۹۲۲۶۴۹۶
DEC	۱۸۰۴	۱۵۶۶	۳۲۰۰	۲۲۸.۳۳۲	۲.۹۲۲۶۴۹۴
DECENC	۳۳۱۷	۴۲۶۸	۵۵۵۳	۲۲۸.۳۳۲	۵.۸۴۵۲۹۹۲

جدول ۱۶) سنتز معماری تکراری پایه‌ای با روش پیشنهادی استفاده از سخت‌افزار XC7285TL-1LFFG1157 بهینه شده برای حجم

ماژول	SLICE	FLIP-FLPO	LUTS	FREQUENCY (Mhz)	Z(bps)
ENC	۱۲۹۷	۱۲۵۲	۱۰۱۶	۴۶۰.۳۴۲	۵.۸۹۲۳۷۷۶
DEC	۱۵۵۳	۲۰۱۹	۱۳۱۴	۴۶۳.۳۲۸	۵.۹۳۰۵۹۸۴
DECENC	۴۲۴۰	۳۳۶۹	۲۸۱۶	۴۶۳.۳۲۸	۱۱.۸۶۱۹۶۸

نتیجه‌گیری

در معماری‌های موجود پیاده‌سازی ماژول تولید و بسط کلید کدر و دیکدر در دو سخت‌افزار کاملاً جدا ازهم اجرا می‌شود. این روش با تأخیر و افزایش حجم سخت‌افزار و افزایش توان مصرفی مواجه است. ولی در روش پیشنهادی فقط یک ماژول برای تولید و بسط کلید کدر و دیکدر طراحی می‌گردد. با بررسی جداول بالا به نتایج زیر می‌رسیم

۱- در ردیف اول تمامی جداول بالا کدر AES و در ردیف دوم دیکدر AES به روش متداول، اجرا و در برنامه ISE شبیه‌سازی و درسه نوع FPGA در دو وضیعت بهینه برای سرعت و حجم جانمایی شده است.

۲- در ردیف سوم تمامی جداول بالا اجرای کُدر و دیکُدر AES به روش پیشنهادی این مقاله در برنامه ISE شبیه سازی و درسه نوع FPGA در دو وضیعت بهینه برای سرعت و حجم جانمایی شده است. در روش پیشنهادی هر دو سخت‌افزار کدر و دیکدر با استفاده از یک ماژول بسط و توسعه کلید طراحی و جانمایی شده‌اند. با بررسی اعداد و ارقام مندرج در این جدول که از خروجی برنامه ISE به‌دست آمده است نتایج زیربه‌دست می‌آید

الف- در صورتی که شبیه‌سازی برنامه، برای سرعت بهینه شده‌باشد حجم و سرعت اجرای سخت‌افزار مورد نیاز برای جانمایی در FPGA بالا می‌رود. این وضعیت برای کاربردهایی که

سرعت بالا برای اجرای برنامه مورد نظر است و محدودیت انرژی وجود نداشته باشد مناسب است.

ب- در صورتی که شبیه‌سازی برنامه، برای حجم بهینه شده‌باشد حجم و سرعت اجرای سخت‌افزار مورد نیاز برای جانمایی در FPGA پایین می‌آید. این وضعیت برای کاربردهایی که محدودیت انرژی و محدویت سخت‌افزار وجود داشته باشد مناسب است.

ج- در صورتی که شبیه‌سازی برنامه، بر اساس روش پیشنهادی این مقاله باشد؛ حجم سخت‌افزار مورد نیاز برای جانمایی در FPGA بالا می‌رود ولی سرعت اجرای برنامه تغییر نمی‌کند اما گذردهی مدار که یک پارامتر مهم در طراحی کدر و دیکدر است بالا می‌رود این وضعیت برای کاربردهایی که محدودیت انرژی و محدویت سخت‌افزار وجود نداشته باشد مناسب است.

روشی که در این مقاله به عنوان پیشنهاد ارائه و مورد تجزیه و تحلیل قرار گرفت، اجرای یک ماژول برای تولید و بسط کلید مورد نیاز کدر و دیکدر است. مزایای روش پیشنهادی به شرح زیر است:

افزایش گذردهی سامانه به میزان تقریبی دو برابر

اجرای هم زمان و بدون تأخیر کُدر و دیکُدر

اعمال یک کلید رمز برای هر دو سخت افزار کُدر و دیکُدر

پیشنهاد

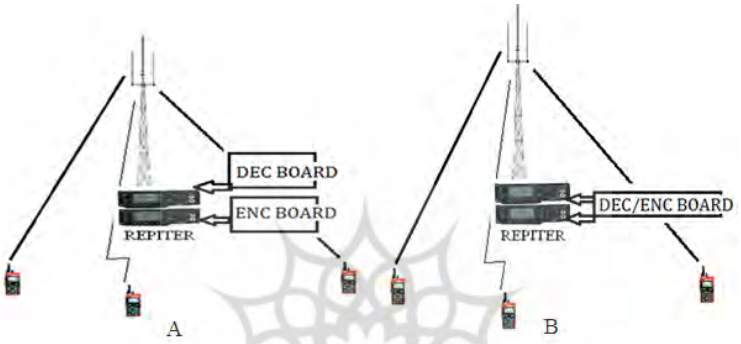
در این مقاله روش پیشنهادی فقط برروی معماری تکراری پایه‌ای بررسی گردید. معماری‌های دیگری نیز برای پیاده‌سازی الگوریتم رمز AES وجود دارد که برخی از آنها به ترتیب معماری خط‌لوله‌ای یک مرحله‌ای و معماری خط‌لوله‌ای چهارمرحله‌ای است.

پیشنهاد می‌شود روش مورد اشاره در این مقاله در سایر معماری‌ها نیز مورد بررسی قرار گیرد.

نتایج حاصل از این مقاله که در بهبود مدارات رمز تجهیزات رادیویی تأثیر بسزایی دارد می‌تواند در تجهیز انواع بی‌سیم‌های مرکزی و تکرارکننده‌ها در بخش‌های نظامی و غیر نظامی کاربرد داشته‌باشد. آنچه که در این مقاله به آن تاکید بیشتری گردیده است استفاده از رمزکننده پیشنهادی در تکرارکننده‌های رادیویی است. در حال حاضر در این تکرارکننده‌ها از دو برد کاملاً مجزا برای رمز و کشف رمز استفاده می‌شود که باعث بالا رفتن هزینه‌های اولیه و جاری و کاهش سرعت انجام عملیات رمز می‌گردد. در صورتی که اگر از

نتایج این مقاله در طراحی رمزکننده برای تجهیزات رادیویی مخصوصاً تکرارکننده‌ها استفاده شود هزینه‌های اولیه و جاری به مراتب پایین می‌آید و عملیات رمز وکشف رمز پیام‌های رادیویی با سرعت بالاتری انجام می‌گیرد. شکل (۱۳-A) روش متداول اجرای رمزکننده در تکرار کننده‌های رادیویی و شکل (۱۳-B) روش پیشنهادی برای اجرای رمزکننده در تکرارکننده‌های رادیویی را نمایش می‌دهد.

شکل ۱۳) تجهیز تکرارکننده‌های رادیویی به برد رمزکننده A روش متداول و B روش پیشنهادی



منابع و ماخذ

- سمیعی، هادی، پایان‌نامه کارشناسی ارشد پیاده‌سازی الگوریتم AES در سخت‌افزار FPGA برای خطوط تلفن- دانشگاه هوایی شهید ستاری- شهریور ۱۳۸۶
- منصوری، کیوان، پایان‌نامه کارشناسی ارشد پیاده‌سازی الگوریتم AES در سخت‌افزار FPGA– دانشگاه صنعتی مالک اشتر- شهریور ۱۳۸۸

- National Institute Of Standards And Technology (U.S.), Advanced Encryptionstandard. Available At: Http://Csrc.Nist.Gov/Publication/Drafts/Dfips-AES.Pdf
- Douglas R.Stinson, " CRYPT OGRAPHY – Theory and Practice ", Second Edition, Waterloo Ontario.
- Viktor, Fischer, Realization Of The Round 2 AES Candidates Using Altera FPGA
- MICRONIC S. R. O., Dunajská 12, Košice, Slovakia Www.Micronic.Sk
- Hamid Jafar Khani,"Spase-Time Coding Theory And Practice",Cambridge Univercity Press 2005
- Rajender Manteena By Major Professor: Wilfrido Moreno, Ph.D. James Leffew, Ph.D. Wei Qian, Ph.D, A Vhdl Implemetation Of The Advanced Encryption Standard-Rijndael Algorithm. Department of Electrical Engineering College of Engineering University of South Florida Date Of Approval: March 23, 2004

- Samiee, Hadi, A Novel Area-Throughput Optimized Architecture for the AES Algorithm, International Conference on Electronic Devices, Systems and Applications (ICEDSA) 2010 IEEE
- J.Org J. Buchholz, Matlab Implementation Of The Advanced Encryption Standard Http://Buchholz.Hs-Bremen.De December 19, 2001
- Suresh,Gyan Vihar,Pallavi Atha, Design & Implementation Of Aes Algorithm Over Fpga Using VhdL, Electronics & Communication University Mahal Jagatpura Jaipur, Rajasthan India,
- International Journal of Engineering, Business and Enterprise Applications (IJEBEA), 2013, Ije Bea All Rights Reserved
- Pallavi Atha, Suresh, Gyan,Vihar,An Improved Aes S-Box And Its Performance Analysis Chia University Taichung 40724, Taiwan Alan3c@Gmail.Com Received January 2010; Revised May 2010
- M. Komala Subhadra,Advanced Encryption Standard - VHDL Implementation, Department Of Electronics And Communication Engineering, Sree Nidhi Institute Of Science And Technology(SNIST) Hyderabad, Andhra Pradesh, Ind 3, November – 2013
- Xinmiao Zhang, Student Member, High-Speed VLSI Architectures For The AES Algorithm, IEEE, And Keshab K. Parhi, Fellow, IEEE, IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, VOL. 12, NO. 9, SEPTEMBER 2004
- - Marcelo B. De Barcelos Design Case, "Optimized Performance And Area Implementation Of Advanced Encryption Standard In Altera Devices, By, Http://Www.Inf.Ufrgs.Br/~Panato/Artigos/Designcon0
- Meghana Hasamnis, Priyanka Jambhulkar-Implementation Of Aes As A Custom Hardware Using Nios Ii Processor Advanced Computing: An International Journal (Acij), Vol.3, No.4,