

## چکیده

هدف از این پروژه مقایسه چهار طرح ضرب کننده RNS می باشد. بدین منظور با بهره گیری از پیاده سازی این چهار طرح با نرم افزار VHDL به مقایسه آنها می پردازیم. RNS یک روش نمایش اعداد است که در آن هر عدد به وسیله باقی مانده های تقسیم آن بر مجموعه ای از اعداد دو به دو نسبت به هم اول نمایش داده می شود. با کمک قضیه باقی مانده چینی، اثبات می شود که در RNS نمایش هر عدد منحصر به فرد می باشد برای ضرب در RNS نیاز به ضرب پیمانه ای خواهد بود. روشهای ضرب پیمانه ای برحسب اینکه کاهش به پیمانه، در کدام مرحله ضرب انجام گیرد. به دو دسته «کاهش در حین ضرب (RDM)» و «کاهش بعد از ضرب (RAM)» تقسیم می شوند. دو طرح اول این پروژه با تکنیک RAM و دو طرح دوم با تکنیک RDM کار می کنند.

## فهرست مطالب

صفحه	عنوان
۱- مقدمه..... ۱	۱- مقدمه..... ۱
۱-۱ سیستم عددی باقیمانده..... ۱	۱-۱ سیستم عددی باقیمانده..... ۱
۲-۱ قضیه باقی مانده های چینی..... ۲	۲-۱ قضیه باقی مانده های چینی..... ۲
۳-۱ کاربردهای RNS..... ۳	۳-۱ کاربردهای RNS..... ۳
۲- روشهای ضرب پیمانه ای..... ۵	۲- روشهای ضرب پیمانه ای..... ۵
۱-۲ روش مونتگمری..... ۵	۱-۲ روش مونتگمری..... ۵
۲-۲ بررسی اجمالی روشهای موجود پیاده سازی ضرب در RNS..... ۶	۲-۲ بررسی اجمالی روشهای موجود پیاده سازی ضرب در RNS..... ۶
۳-۲ نکاتی پیرامون چهار طرح مورد نظر..... ۷	۳-۲ نکاتی پیرامون چهار طرح مورد نظر..... ۷
۳- طرح اول..... ۸	۳- طرح اول..... ۸
۱-۳ مقدمه..... ۸	۱-۳ مقدمه..... ۸
۲-۳ بررسی سوابق..... ۸	۲-۳ بررسی سوابق..... ۸
۳-۳ الگوریتم..... ۹	۳-۳ الگوریتم..... ۹
۴-۳ پیاده سازی سخت افزاری..... ۱۰	۴-۳ پیاده سازی سخت افزاری..... ۱۰
۵-۳ محاسبه پیچیدگی مساحت و تأخیر طرح اول..... ۱۳	۵-۳ محاسبه پیچیدگی مساحت و تأخیر طرح اول..... ۱۳
۴- طرح دوم..... ۱۵	۴- طرح دوم..... ۱۵

- ۴-۱ مقدمه ..... ۱۵
- ۴-۲ بررسی سوابق ..... ۱۵
- ۴-۳ الگوریتم ..... ۱۵
- ۴-۴ پیاده سازی سخت افزاری ..... ۱۸
- ۴-۵ محاسبه پیچیدگی مساحت و تأخیر طرح دوم ..... ۲۰
- ۵- طرح سوم ..... ۲۱
- ۵-۱ تبدیل سیستم RNS (Residue Conversion) ..... ۲۸
- ۵-۲ پیاده سازی سخت افزاری ..... ۳۰
- ۵-۲-۱ پیاده سازی تبدیل RNS ..... ۳۱
- ۵-۲-۲ پیاده سازی بخش اصلی الگوریتم (الگوریتم مونتگمری با RNS) ..... ۳۴
- ۵-۳ محاسبه پیچیدگی مساحت و تأخیر طرح سوم ..... ۳۶
- ۵-۳-۱ عناصر وابسته به ROM ..... ۳۶
- ۵-۳-۲ عناصر ریاضی ..... ۳۶
- ۵-۳-۳ تأخیر و مساحت تبدیل کننده RNS استاندارد ..... ۳۷
- ۵-۳-۴ محاسبه مساحت و تأخیر تبدیل کننده RNS سریع ..... ۴۴
- ۵-۳-۵ مساحت و تأخیر طرح سوم ..... ۵۰
- ۵-۴ نتایج پیاده سازی در طرح سوم ..... ۵۶
- ۶- طرح چهارم ..... ۵۸

۱-۶ بیان مقاله در مورد سیستم RNS ..... ۵۹

۲-۶ بیان مقاله از ضرب پیمانه ای بدون تقسیم (روش مونتگمری) ..... ۶۰

۳-۶ بررسی صحت الگوریتم ..... ۶۲

۴-۶ روش تبدیل RNS ..... ۶۶

۵-۶ پیاده سازی سخت افزاری ..... ۶۷

۱-۵-۶ تبدیل RNS ناقص ..... ۶۸

۲-۵-۶ پیاده سازی بخش اصلی طرح چهارم (الگوریتم مونتگمری) ... ۶۸

۶-۶ محاسبه پیچیدگی تأخیر و مساحت طرح چهارم ..... ۷۰

۱-۶-۶ محاسبه تأخیر و مساحت تبدیل RNS ناقص ..... ۷۰

۲-۶-۶ محاسبه تأخیر و مساحت در طرح چهارم ..... ۷۲

۷-۶ نتایج شبیه سازی در طرح چهارم ..... ۸۰

۷- مقایسه طرح ها و جمع بندی ..... ۸۱

۱-۷- مقایسه چهار طرح ..... ۸۱

۲-۷- جمع بندی ..... ۹۸

۸- مراجع ..... ۹۸

۹- ضمائم ..... ۹۸

الف - کدهای VHDL طرح اول ..... ۹۸

ب - کدهای VHDL طرح دوم ..... ۹۸

جهت خرید فایل word به سایت [www.kandooocn.com](http://www.kandooocn.com) مراجعه کنید  
یا با شماره های ۰۹۳۶۶۰۲۷۴۱۷ و ۰۹۳۶۶۴۰۶۸۵۷ و ۰۶۶۴۱۲۶۰-۵۱۱ تماس حاصل نمایید

ج - کدهای VHDL طرح سوم .....

د - کدهای VHDL طرح چهارم .....

هـ - MOMA .....

[www.kandooocn.com](http://www.kandooocn.com)  
[www.kandooocn.com](http://www.kandooocn.com)  
[www.kandooocn.com](http://www.kandooocn.com)