بسمه تعالی **زمان نصب در تابلوی اعلانات:**

عنوان رساله:

کاهش منابع معماری ضرب چندجمله‌ای در رمزنگاری مشبکه مبنا

دانشجو: یحیی ارزانی بیرگانی

استاد راهنما: دکتر سمیه تیمارچی

چکیده:

طرح‌های مشبکه‌مبنا، از محبوب‌ترین طرح‌های پساکوانتومی محسوب می‌شوند. ضرب صحیح–چندجمله‌ای اساسی‌ترین عملگر مورداستفاده در طرح‌های مشبکه‌مبنا است. اغلب پیاده‌سازی‌های انجام‌شده ضرب صحیح–چندجمله‌ای به پیمانه $x^n + 1; n = 2^m$ اختصاص دارند. دلیل محبوبیت این ۲–جمله‌ای، سادگی و کارایی بالای آن است که حاصل انجام عملیات ضرب توسط روش NTT است؛ اما امکان استفاده از این روش تنها منحصر به این ۲–جمله‌ای رایج است. در پژوهش حاضر علاوه بر توجه به ۲–جمله‌ای رایج، با هدف دستیابی به اندازه کلید کوچک‌تر و تنوع امنیتی، ارائه معماری ضرب مبتنی بر پیمانه‌های سیکلوتومی ۳– و ۵–جمله‌ای نیز در دستور کار قرارگرفته است. ازاین‌رو روش Schoolbook به‌عنوان الگوی پایه انتخاب شده است تا، با تکیه‌بر انعطاف‌پذیری آن، بر پیچیدگی‌های ناشی از پیمانه‌های ۳– و ۵–جمله‌ای فائق آییم.

این پژوهش با ارزیابی معماری‌های موجودِ سریال و تمام–موازیِ مبتنی بر روش Schoolbook دریافته است که راهکار ایجاد امکان رقابت‌پذیری با روش NTT از رهگذر ایجاد یک الگوی تناوبی برای عملیات "سفارش‌دهی ضرایب"چندجمله‌ای می‌گذرد. برای این منظور ابتدا با ارائه دو معماری پیشنهادی بسیار سبک‌وزن رمزنگاری متقارن به ارزیابیِ نقاط ضعف و قوت بهره‌گیری از الگوی تناوبِ عملوند در عملیات سفارش‌دهی می‌پردازیم. سپس در اولین گام از دستیابی به یک طراحی انعطاف‌پذیر برای ضرب صحیح–چندجمله‌ای، یک معماری موازیِ مقیاس‌پذیر پیشنهاد می‌شود. در این گام، بر رویکرد "به اشتراک‌گذاری زمان"با قابلیت پشتیبانی از چندین سطح از موازی‌سازیِ جزئی، با استفاده از ۴، ۸، ۱۶ یا ۳۲ بلوک DSP برای پیمانه ۲–جمله‌ای از درجه $n = 256$، تمرکز می‌شود. بهره‌گیری از الگوی تناوبِ عملوند در معماریِ پیشنهادی، موجبِ انعطاف‌پذیری در استفاده از بلوک‌های ضرب–و–انباره و دستیابی به مصالحه مطلوب میان پارامترهای تأخیر زمانی و منابع مصرفی می‌شود. در گام بعد، با ارزیابی ویژگی‌های ضرب مبتنی بر پیمانه‌های سیکلوتومی ۳– و ۵–جمله‌ای، یک سلول پردازشیِ بهینه و یک سلولِ کنترلیِ متناظر با آن پیشنهاد می‌شود. به‌کارگیری این سلول‌های پیشنهادی برای توسعه معماریِ موازیِ مقیاس‌پذیر طراحی‌شده در گام پیشین، در کنار طراحی یک جریانِ داده دو–حالته، منجر به دستیابی به یک معماری سخت‌افزاری با بهبود چشم‌گیر مصالحه سرعت–منابع مصرفی نسبت به معماری‌های سخت/نرم‌افزاری موجود در سیکلوتومی‌های متنوع می‌شود. از سوی دیگر این معماری با ارائه نتایج رقابت‌پذیر با معماری NTT مبتنی بر ۲–جمله‌ای رایج در بازه درجات $128 < n \leq 2048$، می‌تواند نویدبخش چشم‌اندازی روشن در جلب‌توجه بیشتر به پیمانه‌های سیکلوتومی غیر ۲–جمله‌ای در رمزنگاری مشبکه‌مبنا در آینده باشد.

زمان برگزاری: دوشنبه ۱۴۰۱/۰۶/۲۸ ساعت ۱۷:۰۰

مکان برگزاری: دانشکده مهندسی برق، اتاق جلسات طبقه دوم