دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

نام دانشجو: حسین نادری ورندی		نام استاد راهنما: دکتر راضیه سالاری‌فرد
مقطع: کارشناسی ارشد	رشته: مهندسی کامپیوتر	گرایش: معماری کامپیوتر
نوع دفاع: • دفاع پروپوزال □ • دفاع پایان نامه ■ • دفاع رساله دکترا □		تاریخ: ۱۴۰۳/۰۸/۰۹ ساعت: ۹ صبح مکان: کلاس ۱۱۷

عنوان: یک معماری کارا و امن برای الگوریتم پساکوانتومی کایبر با استفاده از هم‌طراحی سخت‌افزار و نرم‌افزار

داوران خارجی: آقای دکتر هادی سلیمانی	داوران داخلی: آقای دکتر سید حسین عطارزاده نیاکی

چکیده:

با ظهور کامپیوترهای کوانتوم و رشد فزاینده آن ها انتظار می روند در سال های آتی از این کامپیوترها استفاده صنعتی شود. از طرفی الگوریتم کوانتومی Shor نشان می دهد مسائل سخت تجزیه و لگاریتم گسسته که مبنای رمزنگاری کلید عمومی کنونی هستند، توسط کامپیوترهای کوانتوم شکسته خواهند شد. بنابراین در سال های گذشته محققین به طراحی رمزنگاری کلید عمومی که نسبت به حملات کوانتومی امن باشند، پرداخته اند. در ادامه این تحقیقات رمزنگاری های متفاوتی ارائه شده که موفق ترین آن ها رمزنگاری های مشبکه مبنا بوده اند. رمزنگاری مشبکه مبنای کایبر یکی از رمزنگاری های پساکوانتومی است که اخیراً توسط مؤسسه ملی فناوری و استانداردها به عنوان استاندارد معرفی شده است. الگوریتم رمزنگاری کایبر به دلیل ذات مشبکه مبنا و پساکوانتومی بودنش بسیار الگوریتم پیچیده ای محسوب می شود. بنابراین ارائه یک معماری کارا و در عین حال امن برای این الگوریتم بسیار ضروری است. از طرفی امروزه به دلیل بهره بردن از مزایای سخت افزار و نرم افزار در کنار یکدیگر، استفاده از بردهایی که مناسب هم طراحی سخت افزار و نرم افزار هستند بسیار رایج شده است. در این پژوهش با هدف ارائه یک معماری هم طراحی سخت افزار و نرم افزار ابتدا یک شبیه ساز طراحی شده است که کل فضای استفاده همزمان از سخت افزار و نرم افزار با در نظر داشتن امنیت کلید خصوصی را جستجو می کند. در نهایت با تحلیل نتایج آن چند نوع معماری کارا انتخاب شده است. در ادامه به منظور حصول به معماری کاراتر ضرب نظریه اعداد که سنگین ترین واحد محاسباتی کایبر محسوب می شود باز طراحی شده است و با ارائه یک الگوریتم کاهش جدید، یک ضرب نظریه اعداد کارا ارائه شده است. در نهایت یک معماری کارا و امن از کل کایبر ارائه شده است. این معماری با استفاده از تراشه MPSoCs +UltraScale Zynq و ابزار Vivadoو Vitis پیاده سازی شده اند. نتیجه پیاده سازی نشان می دهد که معماری پیشنهادی کارا و امن ما نسبت به بهترین کار پیشین مشابه (AT مساحت*زمان) ٪۷۷ بهبود پیدا کرده است. همچنین زمان اجرای کایبر با استفاده از هم طراحی سخت افزار و نرم افزار و معماری پیشنهادی نسبت به پیاده سازی نرم افزاری ٪۳۹ کاهش پیدا کرده است .