دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

نام دانشجو: **فاطمه مرادی حقیقی**		**نام استاد راهنما:** **جناب آقای دکتر جهانیان**
مقطع: کارشناسی ارشد	**رشته: مهندسی کامپیوتر**	**گرایش: معماری سیستم های کامپیوتری**
نوع دفاع: • **دفاع پروپوزال** □ • **دفاع پایان نامه** ■ • **دفاع رساله دکترا** □		**تاریخ: ۱۴۰۲/۶/۲۸** **ساعت: ۱۶-۱۸** **مکان: دانشکده مهندسی و علوم کامپیوتر – اتاق ۱۱۷**
عنوان: ارتقاء امنیت سخت‌افزار نسبت به حملات کانال جانبی مبتنی بر یادگیری عمیق با استفاده از بازپیکربندی پویا		
داوران خارجی: جناب آقای دکتر صفری		**داوران داخلی: جناب آقای دکتر مهدیانی**

چکیده:

در دنیای دیجیتال امروزی، رمزنگاری برای ایمن سازی تراکنش‌های مالی و محافظت از داده‌های حساس استفاده می‌شود و زیربنای اعتماد و امنیت تعاملات دیجیتال است. اگرچه الگوریتم‌های به کار رفته در دستگاه‌های رمزنگار از نظر تئوری ایمن هستند، محدودیت‌های پیاده‌سازی فیزیکی باعث شده تا مهاجمان، همچنان با حملات کانال جانبی، امنیت آن‌ها را به خطر بیندازند. با افزایش قدرت این حملات، نیاز به ایجاد روش‌هایی برای مقابله با آنها افزوده می‌شود. یکی از روش‌های مقابله با حملات کانال جانبی، پیکربندی پویا است که امکان تغییر پیکربندی و عملکرد یک سامانه سخت افزاری را بدون وقفه ممکن می‌سازد. در این پژوهش به بررسی یک الگوریتم رمزنگاری خط لوله و میزان سختی حمله به آن پرداخته شده‌است. الگوریتم‌های خط لوله به‌دلیل موازی سازی عملیات، سرعت و منابع مورد نیاز سخت افزاری را بهینه می‌سازند. این موازی سازی موجب افزایش نویز در الگوهای توان مصرفی اندازه گیری شده و در نتیجه افزایش امنیت رمزنگاری می‌شوند. ما با ترکیب فن پیکربندی پویا و الگوریتم رمزنگاری مبتنی بر خط لوله، به افزایش مقاومت الگوریتم در برابر حملات کانال جانبی می‌پردازیم.

در این پایان‌نامه با ایجاد یک خط لوله پویا که به‌صورت تصادفی با زمان متغیر است، مقاومت سخت‌افزار در مقابل حملات کانال جانبی افزایش داده‌شده‌است. این تکنیک با ایجاد یک مکانیسم پنهان‌سازی، ساختار زمانی سیستم را به‌صورت تصادفی تغییر می‌دهد و سربار حمله کانال جانبی را تا سطح بسیار خوبی افزایش می‌دهد.

نتایج به‌دست آمده نشان دهنده افزایش قابل توجه زمان و تعداد نمونه‌های مورد نیاز برای انجام یک حمله موفق، نسبت به معماری دارای خط لوله بدون اعمال بازپیکربندی است. هم چنین سربار حافظه این معماری نسبت به پژوهش‌های پیشین ۲۴ درصد بهبود داشته است که نسبت به روش‌های مشابه کاهش چشمگیری دارد. در ضمن در این روش نیازی به ایجاد وقفه در خط لوله در هنگام بازپیکربندی نیست. مزیت دیگر این روش این است که از نگاه طراح سطح بالای سیستم شفاف است و لازم نیست طراح سطح بالا، درگیر جزئیات آن شود.