دانشگاه شهید بهشتی

دانشکده مهندسی و علوم کامپیوتر

اطلاعیه دفاع

<table>
<tr><td colspan="2">نام دانشجو: محمدهادی ولوی</td><td>  </td><td colspan="2">نام استاد راهنما: جناب آقای دکتر قاسم جابری پور</td></tr>
<tr><td colspan="2">رشته: مهندسی کامپیوتر</td><td colspan="2">گرایش: معماری سیستم های کامپیوتری</td><td>مقطع: دکتری</td></tr>
<tr><td colspan="3" rowspan="3">نوع دفاع:
• دفاع رساله دکترا</td><td colspan="2">تاریخ:۱۴۰۰/۹/۲۷</td></tr>
<tr><td colspan="2">ساعت: ۱۰-۱۲ صبح</td></tr>
<tr><td colspan="2">مکان: دانشکده مهندسی و علوم کامپیوتر- کلاس ۱۱۷</td></tr>
<tr><td colspan="5">عنوان:توابع غیرقابل تکثیرفیزیکی در فناوری خودکاره‌های سلولی کوانتومی مبتنی بر پردازنده های حسابی</td></tr>
<tr><td colspan="3">داوران خارجی: جناب آقای دکتر صاحب الزمانی و جناب آقای دکتر ابراهیمی آتانی</td><td colspan="2">داوران داخلی: جناب آقای دکتر جهانیان و جناب آقای دکتر مهدیانی</td></tr>
</table>

چکیده:به موازات رشد سیستم‌های اطلاعاتی و ارتباطی، حمله‌های امنیتی در سطوح مختلف سیستمی اعم از سخت افزار، داده و اطلاعات افزایش یافته است. درحال حاضر راه کارهای امنیتی عمدتا مبتنی بر الگوریتم‌ها و تبدیلات ریاضی هستند که راز مشترکی را بین طرف‌های ارتباطی به اشتراک می‌گذارند. ساختارهای امنیتی مبتنی بر کلیدهای عمومی و خصوصی نمونه‌ای از این پیاده‌سازی‌ها می‌باشند. اما به جهت وجود محدودیتهای متعدد، این روش‌ها به تنهائی قادر به تامین امنیت نیستند. حمله‌های موفق انجام شده به سیستمهای امنیتی در سطح فیزیکی شاهد این مدعاست.

از اینرو توجه به استفاده از روش‌های جدید، جهت مقابله با این تهدیدها بیش از پیش مطرح شده است. یکی از راه حل‌های پیشنهادی استفاده از ساختارهای فیزیکی با امنیت ذاتی است که با حداقل هزینه و حداکثر راندمان، دستیابی به اهداف امنیتی را ممکن می‌سازند. توابع غیرقابل تکثیر فیزیکی (PUF) از جمله این ساختارها هستند که با استخراج ویژگی‌های منحصر به فرد و غیر قابل پیش‌بینی از هویت‌های فیزیکی اهدافی چون تولید کلید و ذخیره و استفاده امن از آن را جهت استفاده در الگوریتم‌های امنیتی میسر می‌سازند.

در دهه‌های اخیر فناوری‌های جدیدی برای پیاده‌سازی سیستم‌های رقمی پیشنهاد شده است. یکی از این فناوری‌ها، فناوری نانوی خودکاره‌های سلولی نقطه کوانتومی (QCA) می‌باشد که با دارا بودن ویژگی‌هایی چون مصرف توان پایین، سرعت کلیدزنی و چگالی بالا به عنوان جایگزین مناسبی برای مدارهای CMOSمطرح می‌باشد. هرچند در فناوریCMOS مفهوم PUF بطور گسترده مطالعه و پیاده‌سازی شده است اما به جهت تفاوت ساختاری این فناوری با QCA استفاده مستقیم از ویژگی‌ها و روش‌های استفاده شده درآنجهت اجرای PUF در QCAممکن نیست و سازوکارهای دیگری برای استخراج ویژگی از هویت‌های فیزیکی در این فناوری مورد نیاز است.

در روش پیشنهادی این رساله از ویژگی‌ها و مختصات منحصر به فرد QCA برای اجرای PUF استفاده می‌شود. این روش مبتنی بر نقص‌های کوچک غیر قابل اجتنابی است که به صورت تصادفی در ساخت سلول‌هاومدارهای QCA بوجود می‌آیند. این نقص‌ها باعث اختلال در عملکرد عادی مدار نمی‌شوند اما می‌توانند ویژگی مناسبی برای تولید امضا برای هر دستگاه باشند. برای این منظور روشی جدید برای کشف نقص و تعیین بزرگی آن درQCA ارائه شده که به صورت موثر نقص‌های کوچک را شناسایی کرده و از آنها برای تولید امضا و پیاده‌سازی PUF استفاده می‌کند. مقایسه نتایج بدست آمده با کارهای مشابه انجام شده که عمدتا در فناوری CMOS هستند نشان می‌دهد که امضاهای تولید شده به خوبی دارای ویژگی‌های لازم برای پیاده‌سازی PUF می‌باشند.