Delay Based PUF for Hardware

Security and Trust

امنیت سخت افزار امروزه به یک دغدغه مهم تبدیل شده است.

از آنجایی که امنیت سخت افزار نیازمند عبور از پروسه های گوناگون میباشد این احتمال وجود دارد که مدار های مخربی توسط افراد سودجو ارائه بشوند.

همچنین برای جلوگیری از دسترسی غیرمجاز افراد مختلف به IC به منظور خواندن داده ها و حتی دستکاری آن ها توابع تکثیر ناپذیر فیزیکی یا PUF معرفی شدند.

PUF پاسخی منحصر به فردی به هر ورودی اعمال شده دارد بطوریکه به راحتی قابل آزمایش و سنجیدن میباشد و از طرفی نمیتوان آن را براحتی تکثیر کرد.

ساختار ها و معماری های متفاوتی از PUF برای ASIC ها و FPGA ها در جهت بهبود معیارهای متفاوتی مانند میزان یکتایی و یکنواختی ارائه شدند.

اما حداکثر میزان یکتایی حاصل از این ساختار ها تنها 40% میباشد.

اما در این مقاله ما PUF را ارائه میدهیم که CRP های متعددی را در جهت بهبود یکتایی تولید میکند.

این PUF ترکیبی از FF APUF و XOR PUF میباشد.

این PUF بر روی FPGA های ورتکس ۶ , اسپارتان ۶ و اسپارتان ۳ پیاده سازی شده است.

که میزان یکتایی محاسبه شده برای هر کدام از این برد ها به ترتیب 46% , 48% , 43% میباشد.

که این میزان در مقایسه با FF APUF پیاده سازی شده بر روی همین برد ها به ترتیب 14% , 7% , 16%

بیشتر میباشد.