بخش اول

معرفی

تلاش برای دستیابی به افزایش قابلیت اطمینان طراحی های سخت افزاری همواره در حال رشد بوده است.

از آنجایی که طراحی و ساخت مدار نیازمند شرکت افراد مختلف می باشد تضمین این واقعیت که سخت افزار مدار دچار دستکاری نشود بسیار بعید می باشد.

می توان گفت که امنیت سخت افزار بطور رسمی بعد از ظهور پدیده تروجان [1]های سخت افزاری معرفی شد.

بسیاری از تکنیک های شناسایی تروجان [2]ها در مراحل بعد از ساخت سیلیکونی معرفی شدند.

که تاکید بیشتر این روش ها بر روی تست و تکرار آن در همان مراحل بعد ساخت می باشد.

اما بجای شناسایی این گونه تهدیدات در مدار های آلوده طبق دستورالعمل[3] بهتر است از ورود این گونه مدار ها در دستگاه مربوطه پیشگیری شود چرا که باعث افزایش قابلیت اطمینان و امنیت میشود.

که به همین منظور در جریان طراحی یا design flow روش ها و متد های گوناگونی پیشنهاد شد[4].

به علاوه جلوگیری از دسترسی غیر مجاز افراد مختلف به داده های مربوط به IC۱ نیز امری بسیار ضروری محسوب میشود.

در نتیجه کلیدی برای دسترسی به داده ها تعبیه شد, تنها افرادی قادر به دسترسی این داده ها هستند که این کلید را در اختیار دارند.

این مفهوم در قالب مراحل توسعه دستگاه با نام Physical Random Function معرفی شد[4].

این مفهوم بعد ها در قالب PUF ۱ تکامل پیدا کرد[5].

PUF ها به گونه ای توسعه پیدا کردند که بتوان از وجود بخش های مختلف سخت افزاری در یک مدار بیشترین بهره وری را داشت.

این بخش های مختلف سخت افزاری میتواند شامل ویژگی های سخت افزاری , تاخیر گیت ها , آستانه ی ولتاژ , ویژگی های الکتریکی ) مقاومت , ظرفیت , اندوکتانس( و ویژگی های نوری و بصری بشود.

ممکن است تفاوت هایی در این بخش ها هنگام ساخت سخت افزار رخ بدهد[6].

اینگونه تفاوت ها نمیتوانند برای دو دستگاه یکسان باشند مانند اثر انگشت انسان ها , پس PUF ها تمرکز خود را به گونه ای معطوف این امر کرده اند که بتوانند این تفاوت ها را شناسایی و حتی در مواردی آن ها را تشدید کنند.

این کارکرد به صورت یک تابع با عنوان PUF به مدار مربوطه اضافه شد.

PUF ها در شاخه های گوناگونی بر اساس ساختار فیزیکی آن ها ) سیلیکونی بودن یا نبود ( , توپولوژی و ... دسته بندی شده اند.

میتوان PUF ها را نیز بر اساس قوی یا ضعیف بودن تقسیم کرد

PUF های قوی دارای CRP۱ های بیشتری هستند و بیشتر برای عملیات شناسایی و احراز هویت بکار میروند.

در حالیکه PUF های ضعیف بیشتر در جهت تولید کلید بکار میروند.

بر اساس ساختار, PUF های سیلیکونی را میتوان در قابلیت هایی مانند تاخیری , حافظه ای و آنالوگ دسته بندی کرد.

در طرف مقابل PUF های غیر سیلیکونی را میتوان در قابلیت هایی مانند نوری , مغناطیسی و آکوستیک را دسته بندی کرد[7].

این ساختار ها توسط نرم افزار ها پیادی سازی شده اند. همچنین ساختار های جدایی برای FPGA[8] و ASIC [9] ها ارائه شده است.

پیاده سازی PUF بر روی FPGA خود نیز دارای چالش های فراوانی میباشد.

باید مراقب باشیم تا از تاثیر مسیریابی۱ یکنواخت جلوگیری شود تا خللی در فرآیند پیاده سازی PUF ایجاد نشود.

در بین این ساختار های معرفی شده PUF های که ساختار آن ها بر اساس تاخیر یا delay میباشند نسبتا قدرتمندتر میباشند .

ازین ساختار ها میتوان به FF APUF[12] , FF PUF[11], APUF[10] اشاره کرد که به توضیح آن ها خواهیم پرداخت.

عملکرد این ساختار ها بر اساس معیار هایی مانند یکتایی یا Uniqueness و قابلیت اطمینان آن ها محاسبه می شود.

همچنین با هم ساختار XOR FF APUF را نیز بر روی خانواده ای از FPGA ها بررسی میکنیم.