انجمن رمز ایران
Iranian Society of Cryptology

پیاده سازی امن الگوریتم های رمزنگاری روی بستره FPGA

تراشه‌های برنامه پذیر مانند FPGAها به عنوان یکی از بسترهای پردازشی محبوب طراحان و مشتریان صنایع دیجیتال مطرح هستند. FPGAها از یک سو سطح بالایی از انعطاف پذیری را در اختیار طراحان قرار می‌دهند که در تراشه‌های خاص منظوره وجود ندارد و از سوی دیگر توان موازی‌سازی قابل توجهی دارند که در کاربردهای پردازش سریع بسیار مهم است. تفاوت بارز این تراشه‌ها با تراشه‌های خاص منظوره این است که با رشته بیتی برنامه ریزی می‌شوند و تغییر رشته بیتی برنامه ریزی و در نتیجه کارکرد آنها را تغییر می‌دهد.

این تراشه‌ها در کنار مزایای بارزی که دارند، از نظر امنیتی دارای مشکلات جدی هستند. در واقع قابلیت برنامه ریزی با رشته بیتی از یکسو انعطاف FPGAها را بالا می‌برد و از سوی دیگر یک گلوگاه امنیتی ایجاد می‌کند. چرا که دسترسی به رشته بیتی و امکان دستکاری آن باعث تغییر کارکرد تراشه FPGA می‌شود.

در این کارگاه روشهایی برای بهبود امنیت طرح نگاشت شده روی FPGA ارائه می‌گردد. روشهای ارائه شده به دو دسته زیر تقسیم می‌شوند:

- **ایجاد امنیت با قابلیتهای بستره:** در این روشها با استفاده از قابلیتهای امنیتی تراشه‌های FPGA مدرن سعی می‌شود امنیت طرح افزایش یابد. روشهایی مانند استفاده از رشته بیتی رمز شده و PUF نمونه هایی از امکانات FPGAهای جدید هستند که مورد بحث قرار خواهند گرفت.
- **طراحی امن روی FPGA:** در این رویکرد، سعی می‌شود با استفاده از تکنیکهای امنیت سخت‌افزار، طراحی به صورتی انجام گیرد که دستکاری آن مشکلتر شود یا در صورت دستکاری، تشخیص آن ساده‌تر باشد.

در این کارگاه نیم‌روزه هر دو رویکرد فوق مورد بحث قرار می‌گیرند و راه‌کارهای عملی به همراه روش استفاده از ابزارهای موجود برای هر راهکار ارائه می‌گردد.