به نام خدا

معماری کامپیوتر

نیمسال دوّم ۰۴-۰۳

استاد: جناب آقای دکتر حسینی منزّه
دستیار استاد: محمدجواد جلیلوند

دانشکده مهندسی کامپیوتر

تمرین سوّم | **VHDL** | مهلت ارسال: ۱۵ فروردین

- مهلت ارسال پاسخ تا ساعت ۲۳:۵۹ مشخص شده است.
- هم‌کاری و هم‌فکری در انجام تمرین مانعی ندارد اما پاسخ ارسالی هر فرد باید توسط خود او نوشته شده باشد.
- در صورت هم‌فکری یا استفاده از منابع خارج از درس، نام هم‌فکران و آدرس منابع مورد استفاده را ذکر کنید.
- برای دریافت نمره کامل هر سوال نیاز است تمامی روابط و فرمول‌ها نوشته شده و توضیحات تشریحی کامل داده شود.
- برای هر کدام از سوالات، کد VHDL و Testbench، به همراه یک گزارش کلی از نحوه انجام هر سوال و شکل خروجی آن‌ها (simulation) تهیه شود.
- لطفاً تصویری واضح از پاسخ سوالات نظری بارگذاری کنید. در غیر این صورت پاسخ شما تصحیح نخواهد شد. (برگه پاسخ سوالات نظری به صورت حضوری دریافت می گردد.)
- سوال اول برای دانشجویان با شماره دانشجویی فرد و سوال دوم برای دانشجویان با شماره دانشجویی زوج است.
- پاسخ تمام سوالات را در یک فایل فشرده به صورت CA_Hw3_[firstName]_[lastName]_[StudentId] نامگذاری کرده و ارسال کنید.

مقدمه

بوت امن (Secure Boot) یک ویژگی امنیتی است که برای محافظت از فرآیند راه‌اندازی کامپیوتر طراحی شده است. این ویژگی اطمینان حاصل می‌کند که تنها نرم‌افزارهای مورد اعتماد (که توسط سازنده یا کاربر تأیید شده‌اند) در هنگام راه‌اندازی سیستم اجرا شوند. با استفاده از امضای دیجیتال، بوت امن تضمین می‌کند که هیچ تغییری در اجزای اصلی بوت (مانند هسته سیستم‌عامل) صورت نگرفته است. این امر به جلوگیری از اجرای کدهای مخرب در مراحل اولیه راه‌اندازی کمک می‌کند.

شرح پروژه

ابتدا الگوریتم تولید هش MD5 [1] را به زبان VHDL پیاده‌سازی کنید. این الگوریتم ورودی را بصورت سریالی دریافت کرده و یک مقدار هش ۱۲۸ بیتی تولید می‌کند. توجه داشته باشید که پیاده‌سازی باید بهینه و قابل اجرا روی سخت‌افزار باشد.

حالا یک ماژول VHDL طراحی کنید که فایل بوت را کلمه [2] به کلمه (هر کلمه ۳۲ بیت) خوانده و این داده‌ها را به الگوریتم MD5 ارسال کند. سپس هش تولید شده را گرفته و با لیست هش‌های مورد اعتماد (که از یک واحد ROM خوانده می‌شوند) مقایسه کند. در صورت انطباق با هریک از آنها، خروجی TRUSTED و در غیر این صورت خروجی ERROR روشن شود.

جزئیات ورودی

لیست هش‌های مورد اعتماد در یک ماژول جداست که از بیرون مدیریت می‌شود و ۱۶ سطر دارد. ماژول شما یک خروجی ۴ بیتی انتخاب سطر و یک ورودی ۱۲۸ بیتی دارد. ماژول تنظیمات، سطر مربوط به شماره انتخاب شده را روی ۱۲۸ بیت ورودی قرار می‌دهد. همچنین فرض کنید حافظه بصورت ۱۶ بیتی آدرس‌دهی می‌شود.

[1] MD5 Hashing Algorithm
[2] word

سوال دوم

مقدمه

شبکه‌های کامپیوتری در کامپیوتر مبدا اطلاعات را به بسته[۳]هایی با اندازه حدودا یک کیلوبایتی تقسیم و به سمت مقصد ارسال می‌کنند. یکی از ساده ترین قطعاتی که در مسیر برای انتقال این بسته‌ها استفاده می‌شود، LAN Switch است. این قطعه دو کار انجام می‌دهد:

- بررسی درست رسیدن بسته: درصورت وجود نویز ممکن است بسته به درستی به سویچ نرسد. در این صورت باید خطا را تشخیص داده و بسته را ارسال نکنیم.
- انتخاب پورت خروجی براساس مقصد موجود در بسته.

شرح پروژه

ابتدا ماژول مربوط به CRC32 را به زبان VHDL پیاده‌سازی کنید. این الگوریتم ورودی را بصورت بیت به بیت دریافت کرده و یک بیت خروجی می‌دهد که نشان‌دهنده معتبر بودن یا نبودن بسته است. توجه داشته باشید که پیاده‌سازی باید بهینه و قابل اجرا روی سخت‌افزار باشد.

حالا یک ماژول VHDL طراحی کنید که بسته را به‌صورت بیت به بیت خوانده، ذخیره و به CRC32 ارسال کند. سپس در صورت معتبر بودن بسته، آدرس مقصد را با لیست تنظیمات مقایسه کند و درصورت پیدا شدن خروجی معتبر، بسته را بصورت بیت به بیت از خروجی مربوطه ارسال کند.

جزئیات ورودی

ساختار بسته ورودی را به این شکل درنظر بگیرید. در ابتدا، مقدار سیم یک است، سپس برای یک کلاک صفر می‌شود و بعد بیت‌های بسته یک به یک (از سمت چپ جدول زیر) دریافت می‌شوند:

	Destination Address	Source Address	Data Length	Data	CRC32
Length	48 bits	48 bits	10 bits	64-1023 bytes	32 bits

بدیهی‌است که قطعات میانی به محتوای بسته‌ها کاری ندارند و فقط بر اساس فیلدهای ابتدا و انتها، ادامه مسیر را مشخص می‌کند. این نوع سویچ، خود فیلدهای ابتدا و انتها را نیز دست‌کاری نمی‌کند و (درصورت تصمیم به ارسال بسته) همه بیت‌های ورودی را بدون تغییر ارسال می‌کند.

جدول تنظیمات در یک ماژول جداست که از بیرون مدیریت می‌شود و ۱۶ سطر دارد. ماژول شما یک خروجی ۴ بیتی انتخاب سطر و یک ورودی ۵۱ بیتی دارد. ماژول تنظیمات، سطر مربوط به شماره انتخاب شده را روی ۵۱ بیت ورودی قرار می‌دهد. ۴۸ بیت اول آدرس مقصد و ۳ بیت آخر شماره پورت خروجی است.

[۳] packet