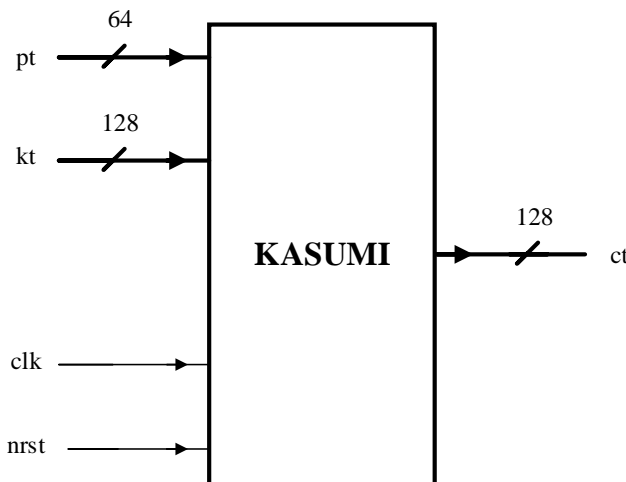


درس طراحی سیستمهای دیجیتال

پروژه نهایی - طراحی پیاده‌سازی الگوریتم رمزنگاری KASUMI

هدف از این پروژه سنتز منطقی و سنتز سطح بالای الگوریتم رمزنگاری KASUMI است که در کاربردهای تلفن همراه به فراوانی استفاده می‌شود. KASUMI یک الگوریتم ساده و سبک برای رمزنگاری بلوکی است که داده ورودی و خروجی آن ۶۴ بیت و کلید رمز آن ۱۲۸ بیت است. ساختار این بلوک به صورت زیر است.



در این ساختار، ورودیهای pt و kt شامل داده خام و کلید هستند و خروجی ct هم داده رمز شده است. ورودی و خروجی بلوکهای ۱۲۸ بیتی و کلید ۶۴ بیتی است. یکبار این الگوریتم را با کد VHDL و در سطح RTL مدل کنید و یکبار آن را با سنتز سطح بالا به صورت خودکار سنتز کنید و سخت‌افزارهای حاصل را از نظر فرکانس، میزان منابع و توان مصرفی مقایسه کنید. در نهایت کد سنتز شده روی FPGA با استفاده از سیستم RemoteFPGA تحویل داده خواهد شد.

به همراه این فایل، کد C الگوریتم و راهنمای ساختار داخلی آن نیز بارگذاری شده است.