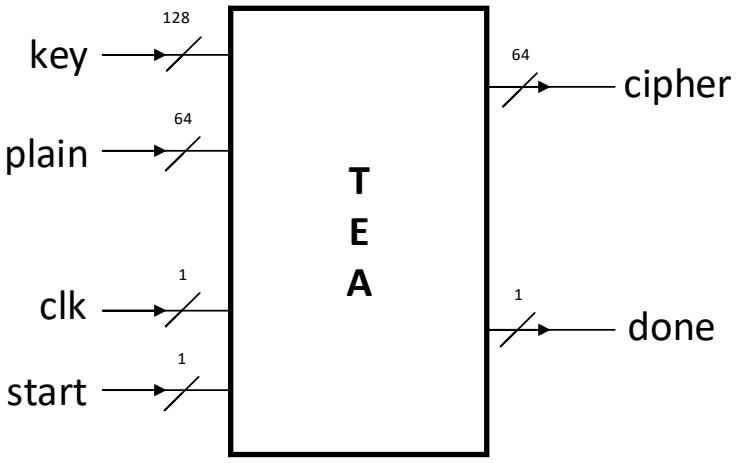
درس طراحی سیسستمهای دیجیتال
پیاده‌سازی الگوریتم رمزنگاری TEA روی FPGA

الگوریتم رمزنگاری Tiny Encryption Algorithm (TEA) یک الگوریتم ساده و سبک برای رمزنگاری بلوکی است. ساختار کلی این رمز کننده به صورت زیر است.



روند کارکرد این سخت‌افزار به این صورت است که هرگاه خط start برابر ’1‘ شود، عمل رمزنگاری شروع می‌شود و داده خام (plain) با استفاده از کلید (key) طی ۳۲ سیکل رمز می‌شود و نتیجه روی داده رمز (cipher) قرار می‌گیرد. در سیکل ۳۲ که داده رمز آماده شده است، خط done برابر ’1‘ می‌شود.

کد نرم‌افزاری این رمزکننده به صورت زیر است.

```
#include <stdint.h>

void encrypt (uint32_t v[2], const uint32_t k[4]) {
   uint32_t v0=v[0], v1=v[1], sum=0, i;          /* set up */
   uint32_t delta=0x9E3779B9;                    /* a key schedule constant */
   uint32_t k0=k[0], k1=k[1], k2=k[2], k3=k[3];   /* cache key */
   for (i=0; i<32; i++) {                        /* basic cycle start */
      sum += delta;
      v0 += ((v1<<4) + k0) ^ (v1 + sum) ^ ((v1>>5) + k1);
      v1 += ((v0<<4) + k2) ^ (v0 + sum) ^ ((v0>>5) + k3);
   }                                             /* end cycle */
   v[0]=v0; v[1]=v1;
}
```

این رمز کننده را با VHDL مدل کرده و روی RemoteFPGA تست کنید.