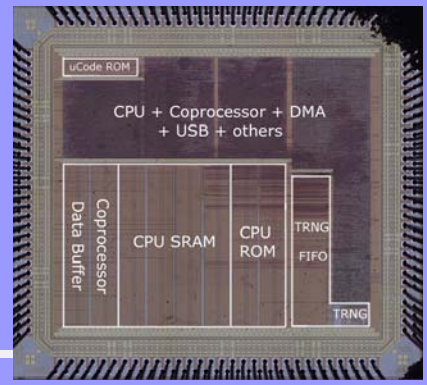
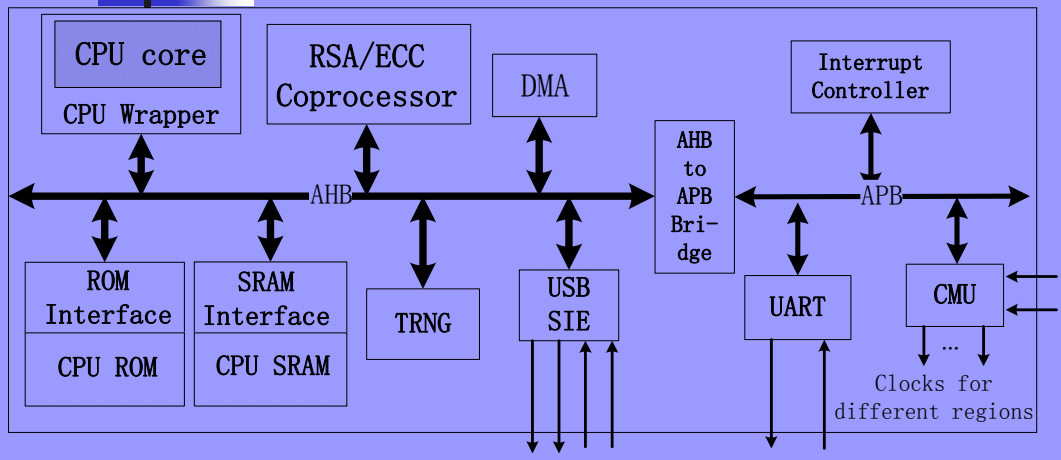
A High-Performance Platform-Based SoC for Information Security

Jun Han
Ph.D student

State Key Lab of ASIC and System, FUDAN University,
Shanghai, China
Tel: +86-21-51355318
Fax: +86-21-51355234
E-mail: 031021025@fudan.edu.cn

SoC Infrastructure

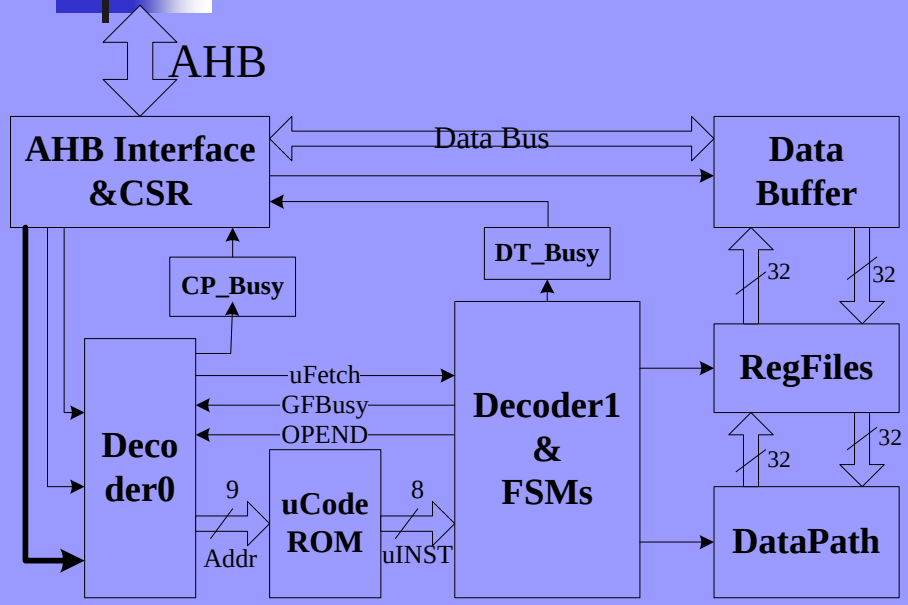




- Chip area: 4.7885*4.3438mm^2 based on TSMC 0.25um process
- Power consumption: 41.6mW@2.5V,30MHz
- Throughput:
  - RSA-1024: 14kbps@2.5v, 30MHz
  - ECC-233: 7.5kbps@2.5v, 30MHz

- 32-bit RISC CPU
- Configurable and Scalable Coprocessor architecture for PKI algorithm such as RSA & ECC
- TRNG for random number generation
- USB 2.0 Serial Interface Engine
- Dynamic Power Management by Firmware
- Special DMA controller for high data throughput

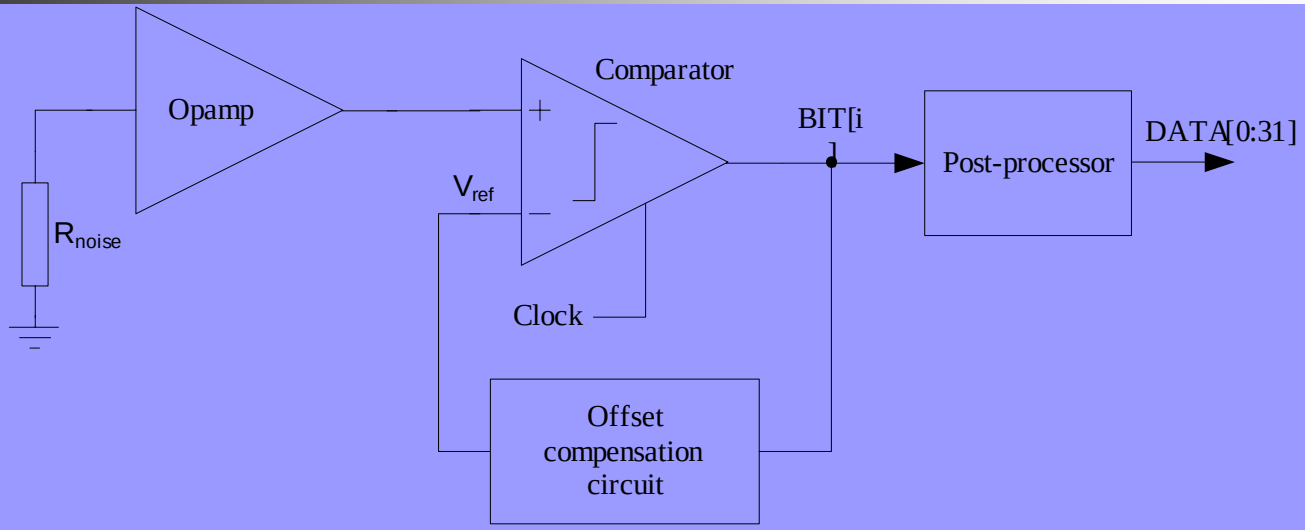
Asymmetric Cryptographic coprocessor



- ✓ Up to 150MHz @TSMC0.25um process
- ✓ about 60K gates @TSMC0.25um process
- ✓14kbps @2.5V, 30MHz for 1024-bit RSA
- ✓7.5kbps @2.5V, 30MHz for 233-bit ECC

- Two stage decoding strategy with micro-instruction structure
- Both RSA and ECC Supported
- 512-bit operand for RSA and 256-bit operand for ECC
- Configurable RSA: 512-bit or 1024-bit
- Configurable ECC: 133-bit, 163-bit, 193-bit and 233-bit
- AHB interface

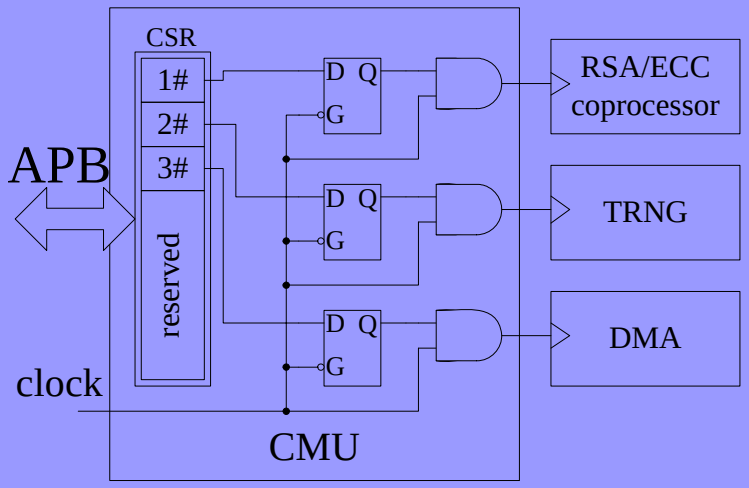
Random Number Generator

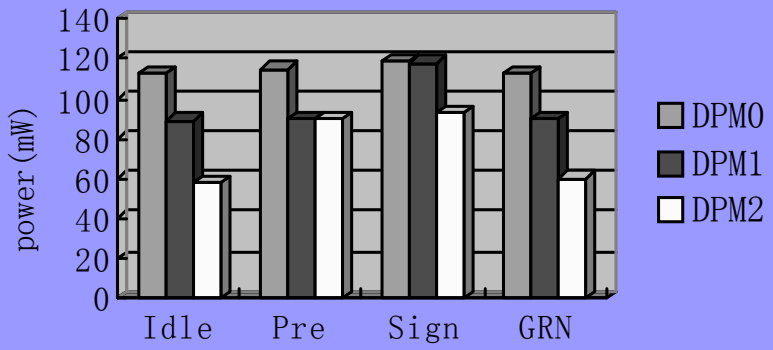


- ✓ Passed NIST FIPS140-1
- ✓ Passed NIST SP800-22

- Based on resistor thermal noise
- Wideband operational amplifier
- offset compensation circuit to remove the offset due to comparator and Op-amp
- Post-processor to enhance the randomicity of TRNG

Low Power Features





- The biggest part of power consumption in 0.25um process: Dynamic Power!
- Cutting down clock supplies for idle blocks
- Firmware to cut/release clock supplies, according to work conditions
- CPU suspend mode
- Glitch free

✓ 21.5% ~ 48.4% power saved according to the operation conditions