DOI:10.19651/j.cnki.emt.2212185

基于高速总线的密码 SoC 设计与实现

王 凯 曲英杰
(青岛科技大学信息科学技术学院 青岛 266061)

摘 要：物联网、汽车制造、智慧医疗等行业的飞速发展，加快了端设备芯片的推广和应用，随之而来的芯片安全问题也暴露出来，传统的单片机或 ARM-A 系列的 CPU 芯片已经不能满足越来越复杂的应用需求。为解决目前端设备存在芯片安全防护不足、传输速度慢、功耗高、计算资源不足等问题，结合 SoC 设计理念，提出了一种基于高速总线的密码 SoC 设计方案，实现对端设备的传感器、芯片、硬件的动态状态获取，接收多种高速协议接口数据，加密存储及备份至云端等功能。该方案基于 SoC 设计，采用开源处理器，完成了一套由处理器、高速总线、硬件外设、加密单元相结合的低功耗加密监控芯片。综合及功耗分析和实验结果表明，实现了数据的高速可靠传输与加密，满足大容量数据快速加解密的需求；采用低功耗设计，性能无影响，功耗降低约 20%。

关键词：芯片设计；高速片内总线；高速数据传输；低功耗设计
中图分类号：TP309.7 **文献标识码**：A **国家标准学科分类代码**：510.4；520.6

Design and implementation of cryptographic SoC based on high speed bus

Wang Kai Qu Yingjie
(School of Information Science & Technology, Qingdao University of Science and Technology, Qingdao 266061, China)

Abstract: The rapid development of industries such as the Internet of Things, automobile manufacturing, and smart medical care has accelerated the promotion and application of end-point-device chips, and subsequent chip security issues have also been exposed. Traditional micro control unit(MCU) or ARM-A series CPU chips can no longer meet the increasingly complex application requirements. In order to solve the problems of insufficient chip security protection, slow transmission speed, high power consumption, and insufficient computing resources in current end devices, combined with the SoC design concept, this paper proposes a cryptographic SoC design scheme based on high-speed bus. This scheme realizes the acquisition of the dynamic status of the sensors, chips, and hardware of the end-device, receiving multiple high-speed protocol interface data, encrypted storage, and backup to the cloud. The solution uses an open-source processor to complete a low-power encryption monitoring chip that combines a processor, a high-speed bus, hardware peripherals, and an encryption unit. Synthesis and power analysis and experimental results show that high-speed and reliable data transmission and encryption are realized to meet the needs of fast encryption and decryption of large-capacity data; low power consumption design is adopted, performance is not affected, and power consumption is reduced by about 20%.

Keywords: chip design; high-speed on-chip bus; high-speed data transmission; low power design

0 引 言

加密芯片是当今保证数据信息安全的重要手段。密码 SoC(system on chip)将通用处理器、密码算法 IP 核、存储和接口模块等单元集成到单颗芯片上，实现数据加解密、消息签名/验证和数据完整性验证等密码应用，已经成为保障信息安全的核心部件[1]。具有安全性强、处理效率高和兼容性强等优势，被广泛应用于数据加密领域。

传统攻击方法对密码芯片的效果一般，但是差分功耗分析(differential power analysis，DPA)攻击技术作为一种获取密码芯片密钥的旁道攻击方法具有较强的攻击性和破解效率[2]。DPA 仅需已知采用哪种算法，并可以采集该算法运行时的功耗信息，即可开展攻击[3]。芯片设计采用低功耗设计，提高功耗的安全性，功耗曲线各时间点上所发生的操作，无法实现真正的对准，差分统计特征较难凸显出来，有效抵御 DPA 攻击，适用于物联网设备芯片。文献[4]

收稿日期：2022-11-24

在核心加解密电路中采用异步控制框架，剔除时钟域，使加密跟寄存器翻转时刻随机化，但在配置的初始化过程，仍然可以从总线至加密核心的传输链路中获取到配置数据的翻转号，不能实现完全的避免 DPA 攻击。文献[5]采用串行外设接口（serial peripheral interface，SPI）协议作为 CPU 与外置加密计算单元的通信接口协议，传输速率低，且安全性较低，并不适合作为加密计算电路的接口协议。文献[6]采用 CPU 作为计算单元，软件实现加密，相比完全硬件实现加密，其运算成本高，资源利用率低，计算速度不快，在迭代成本上存在巨大弊端。密码芯片缺乏低功耗设计、功能应用单一，不符合当前各行各业的需求。

为解决以上问题，本文提出一种基于高速总线的密码 SoC 设计与实现方案。为保证芯片的高可靠性、高兼容性，突破芯片单一总线模式，采用多层异构体系总线技术，实现多时钟域、多设备分层异构系统工作；采用多协议高速数据传输设计，提高数据传输速度，兼容多种高速数据传输协议；加密计算逻辑及芯片架构采用低功耗技术设计，大大降低了芯片各个模式功耗系数。

1　芯片结构设计

1.1　芯片整体结构

芯片的设计需要遵循平衡设计原则，需要在芯片的复杂度、内部结构、性能、功耗、扩展性等各个方面做一定的权衡[7]。在系统级实现架构设计与优化，系统级的设计需要各种在高层次抽象的 IP 来实现[8]。

本设计基于芯片级 SoC 系统架构，实现了芯片各模块的逻辑设计和芯片系统集成及验证。芯片整体划分为 6 个子系统：SoC 核心子系统、加解密子系统、功耗管理子系统、安全启动子系统、高速协议子系统、自动复位子系统。如图 1 所示。

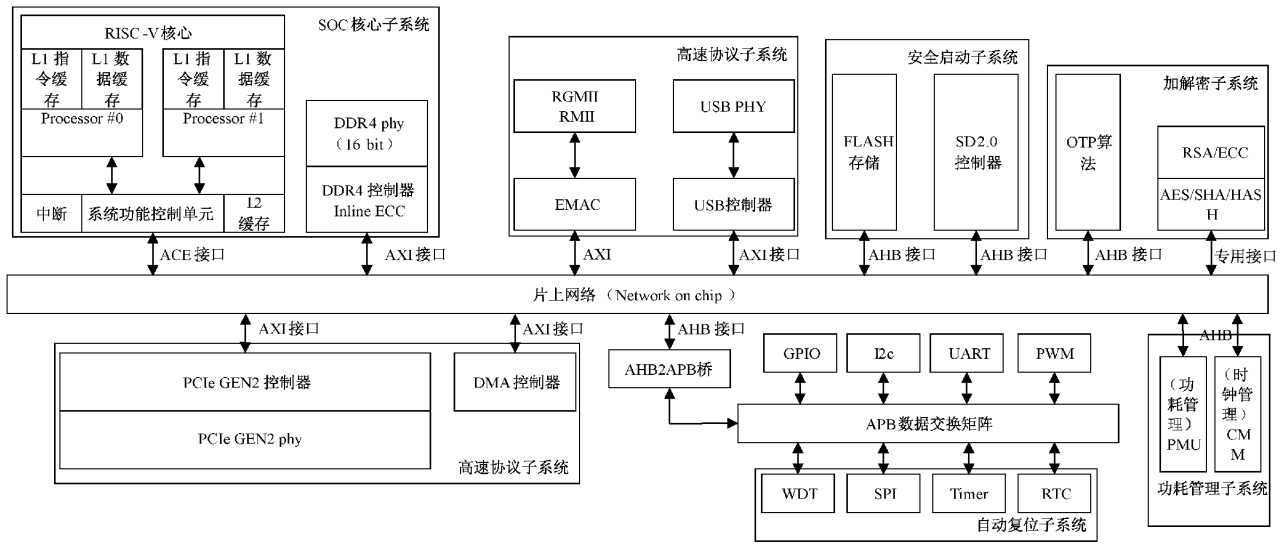

图 1　芯片系统架构

SoC 核心子系统是芯片设计中最重要、最基本的子系统，包括处理器核、系统总线、DDR 控制器、片内存储器等模块；加解密子系统是芯片设计中的运算子系统，包括 RSA/ECC 模块，AES/SHA/HASH 模块，芯片通过该子系统完成各加/解密操作；时钟管理子系统包括时钟管理模块和电源管理模块，完成芯片的时钟、电压供应状况的调整；高速协议子系统用于支持各种高速协议传输数据，内置直接存储器访问（direct memory access，DMA）、分区挂载模块，保证各协议之间数据同时传输，最大程度利用总线带宽；自动复位子系统在系统卡死或者运行程序超时未响应的情况下完成系统的复位动作，主要包括了 TIMER、WDT、UART 等模块。

1.2　内部总线结构

内部总线结构具有可配置、高性能、符合高级微控制器总线架构（advanced microcontroller bus architecture，AMBA）协议的基础架构。网络互联具备可配置功能。如图 2 所示，挂载范围从单个桥组件到 4 个主设备和 16 个从设备组成的复杂互连。

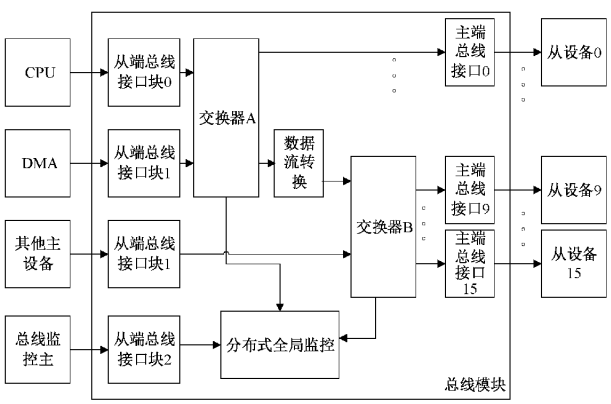

图 2　总线内部结构图

1.3　芯片总线地址划分及主从关系

芯片地址划分如图 3 所示,芯片 CPU 使用的系统总线宽度为 32 bit,系统最大寻址空间为 4 GB。

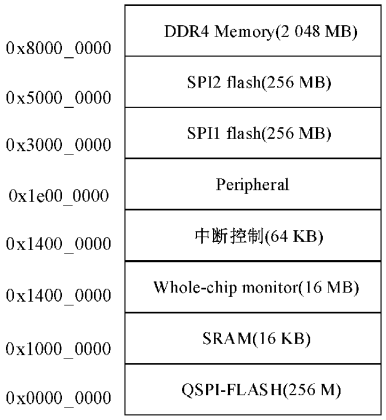

图 3　芯片地址空间划分

片内总线采用 AMBA 总线,用于连接和管理片上系统中的功能模块。AMBA 作为业界开放标准和片上互连规范,具备优秀的可扩展性,可测性等重要指标,深受业界欢迎[9]。

相比文献[10],本文针对高速密集的数据信号,以多协议总线的桥接方式级联,芯片内总线设计采用多层结构,主体总线协议采用 AMBA4 总线体系,使用 APB、AXI、AHB 这 3 层总线协议,在交点位置使用网络互联模块,覆盖高频、中频、低频 3 个区域,完成对各种特性设备的互联和全覆盖。模块分配如表 1 所示。

表 1　总线模块主从分配列表

序列号	模块	总线接口(主设备/从设备)
1	DDR	AXI(从)
2	DMA	AHB(从)/AXI(主)
3	ECC	AHB(从)
4	MAC	AHB(从)/AXI(主)
5	PCIE	AXI(从)
6	SDIO	AHB(从)/AHB(主)
7	SRAM-C	AXI(从)
8	USB	AXI(从)/AHB(从)
9	CPU	AXI(主)
10	其他外设	AXI(从)/AHB(从)/APB(从)

2　芯片关键技术

2.1　加密核高速数据接口

加密核心或通用算法核心,采用总线挂载的方式,具备方便移植、可重用、方便验证与集成的特点,但由于总线频率远低于 CPU 频率,且配置过程需要经过总线链路及桥,读取数据源为远端存储设备,造成执行效率较低;开源的协处理器拓展接口(extension accelerator interface,EAI)接口,接口时序简单易用,但仅能挂载单核或单一算法模块;比对多种实现方式后,设计出一种高速加密核挂载接口,设计框图如图 4 所示,直接从 I-cache 及 D-cache 读取数据,提高数据传递速度,与加密核心使用 opcode(操作码)方式交互,快速区分不同加密核的操作请求;较 EAI 接口,具备多类加密核同时工作的功能特性,执行效率极大提升。

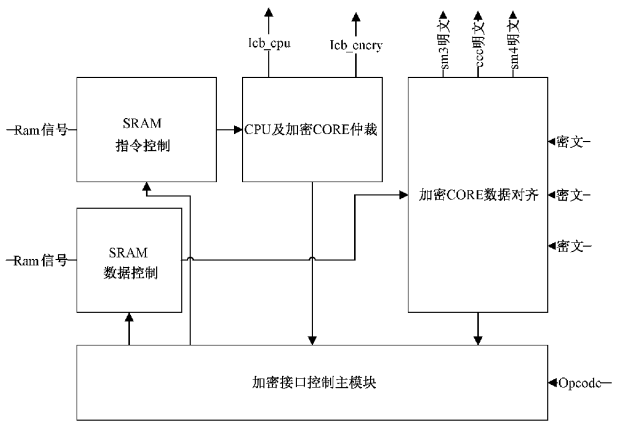

图 4　加密接口设计框图

加密接口设计分为 SRAM 指令控制、SRAM 数据控制、CPU 及加密 CORE 仲裁、加密 CORE 数据对齐、加密接口控制主模块;实现连接 TICM/DTCM SRAM,轮询仲裁请求,识别并读取加密拓展指令并传递给 ENCRY CORE;CORE 解析并发送 opcode 给 MAIN 模块请求;解析 opcode,执行加密数据搬运;ECC/SM3/SM4 core 接口时序及位宽整合;设计框图如图 4 所示,opcode 编解码如表 2 所示,opcode 类型主要为配置、读数据、写回,rsp-done 代表响应结束,hold-up 代表保持响应。

表 2　Opcode 解码表

序列号	Opcode 类型	响应类型(rsp-opcode)
1	Config-1core	Rsp-done/hold-up
2	Read-data	Rsp-done/hold-up
3	Config-2core	Rsp-done/hold-up
4	Config-3core	Rsp-done/hold-up
5	Write-back	Rsp-done/hold-up

模块运行时,加密接口控制主模块的状态跳转如图 5 所示;上电复位后处于空闲状态(IDLE),待 CPU 启动后,主动挂起 ENCRY CORE,加密接口控制主模块由空闲状态进入开始(指令读取)状态,在此阶段若出现低功耗请求,则主动进入空闲状态;读取到 ENCRY CORE 的专用指令后,发送给 ENCRY CORE;CORE 解析指令,回复操作码(opcode);加密接口控制主模块进入解码 & 执行状态,执行操作;进入读取数据或写回状态;完成后返回开始状态。

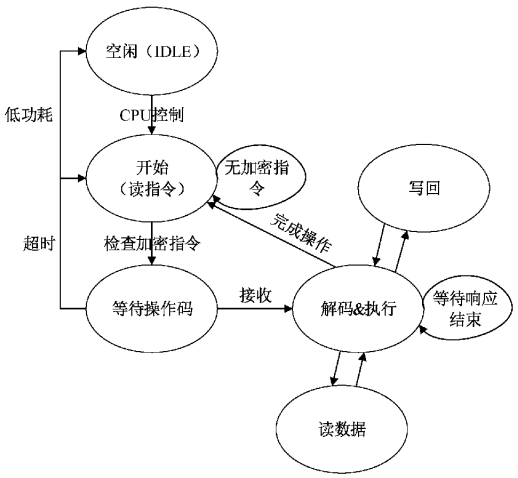

图 5　读数据运行状态图

SM3/SM4 的输入数据为 8 bit 对齐，方便存于内存中，ECC 多项式基、ECC 的基坐标、K 值及参数 b 采用 163 bit 宽度数据，使用并行传输方式，采样数据的整存或整取，会造成至少 5 bit 的数据的浪费问题，此问题同样出现在 ECC 常规挂载总线接口设计方式；本方案分析过后，需要针对单 ECC，及 ECC/SM3/SM4 同时工作的情况区分数据读取方式；单 ECC 工作时，8 bit 对齐，k 及基坐标连续，余 1 bit 数据，7 bit 无效数据；ECC 及其他 core 启动时，后 7 bit 为地址信息偏移，当前地址加后 7 bit 偏移地址，得到 SM3 及 SM4 地址信息，采用非连续存储方式，更好地利用内存空间，防止碎片内存被浪费的情况。

2.2　多协议高速数据传输技术

芯片内部设计多种高速传输协议模块，包括 PCIE、USB、EMAC 等。为保证各种协议正常运行，除设计有各协议功能模块外，采用内置 TileLink 总线协议、IST-DAT DMA 传输技术。架构图如图 6 所示。

TileLink 总线具有以下 4 个特点：1）支持乱序的并发操作以提高吞吐率；2）5 个通道完全独立，利于单独优化时序；3）仅 A/D 两个通道就能完成除缓存一致性相关的所有访存操作，以 opcode 区分具体操作类型，总线利用率较高；4）cache 一致性的内存共享系统，支持兼容 MOESI 的一致性协议[11-14]。

设计 TileLink 总线与 AMBA 桥代理，采用握手结合代理方式，与高速模块的传输层信号交互，利用 opcode 实现高速接口的快速访问，采用多通道结合操作码，实现不同协议传输。

如图 7 所示，DMA-IN 模块，实现 TileLink 总线主端控制，完成高速协议传输的速率、负载、功耗的动态平衡，与 AMBA-DMA 协作，缓解 CPU 指令链路压力。DMA 中配置接口（AHB 从端接口）采用 AMBA AHB 协议。设计通过请求响应及相关握手协议，完成 DMA 流为单个源和目标提供单向串行传输。DMA-IN 通道优先级采用固定

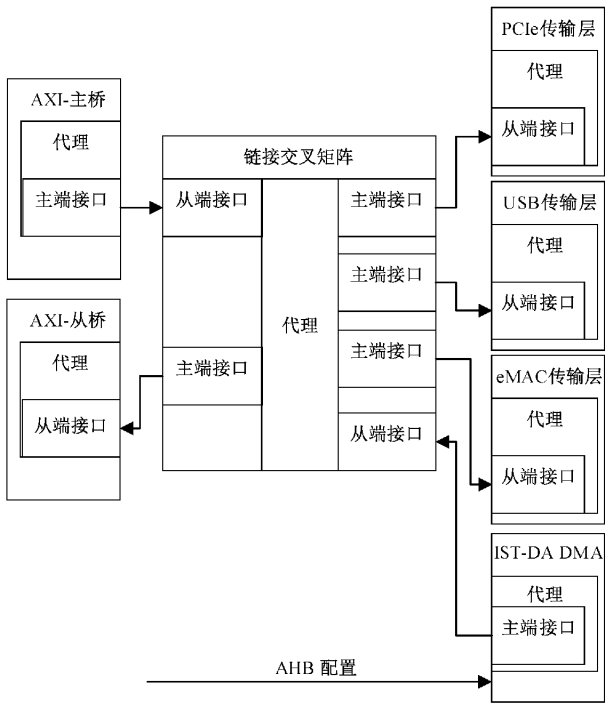

图 6　多协议挂载 TileLink 结构

方式。DMA 中的通道数据路径模块设计成使 AXI 总线饱和，提高利用率。

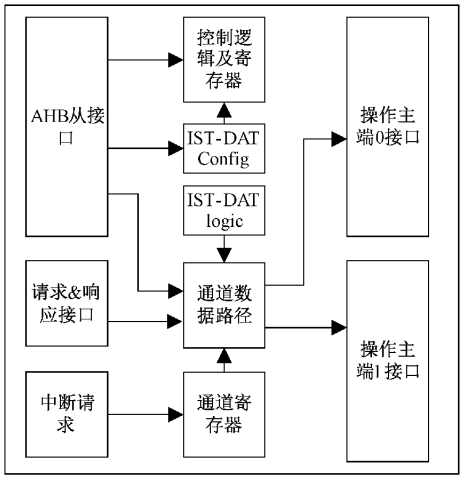

图 7　IST-DAT DMA 模块结构图

时间是影响 DPA 攻击的重要因素，DPA 攻击之所以能够成功，是因为密码设备每次执行的相应运算操作都会出现在固定的时间点上，因此从时间角度对密码设备进行抗 DPA 攻击设计[15]。

IST-DAT（insert data）DMA 传输技术，除 DMA 传输技术外，设计有 IST-DAT 逻辑，如图 8 所示，根据片内 PMU 模块及模块级仿真阶段积累的电平翻转数据，增加插入无效数据功能，平衡翻转功耗，降低了吞吐量，但有效平衡了系统运行时的各模块功耗，且增加了总线时序的随机性（利用 RTC 当前时间产生随机总线时序延迟），在

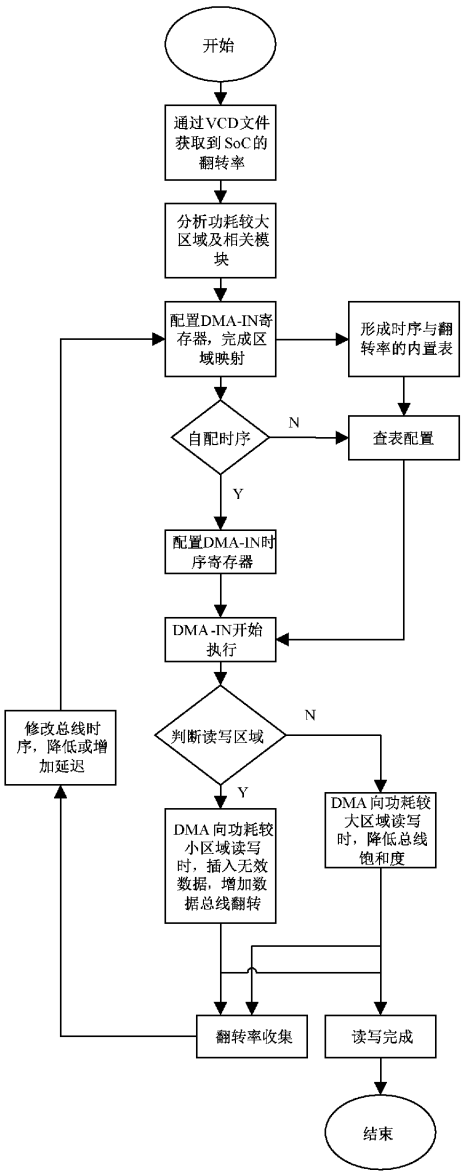

图 8　IST-DAT 流程

opcode 中设计加密单元识别的编码,进行桥接转换时,将其转为特殊 AXI 协议包,使得加密单元在总线无效传输时,可开启无效密钥计算,增强了抵御外部探测硬件数据传输功耗特性的攻击。

2.3　低功耗设计及实现策略

SoC 芯片中通常只有一小部分模块需要长时间保持工作,将其他大部分处于空闲状态的模块关闭时钟或者关闭电源[16]。相比文献[17]中提出从时钟管理角度出发针对 SoC 应用进行的单一设计,密码 SoC 芯片采用多项低功耗技术,包括时钟门控、PMU 功耗管理及 UPF 约束,将其应用于对 AMBA 总线的时钟域管理,实现高低速时钟的动态管理,综合功耗符合芯片设计预期标准。

时钟树功耗包括动态功耗和静态功耗两部分,动态功耗占主要部分[18]。设计采用层次化结合多级分布的门控技术,对于需要控制的寄存器组或逻辑层,加入使能信号,阻止无用的数据进入寄存器组或逻辑层,避免引起无效逻辑翻转,实现功耗降低。

片内 PMU 结构如图 9 所示。芯片设计时,按照功能使用情况,分为了 6 个子系统。PMU 通过 APB 接口,对每个子系统的时钟、复位、电源和隔离单元进行单独控制,同时根据外设地址分步,在 PMU 内置地址映射单元,通过 APB 接口,选择映射的具体模块进行电源、时钟、复位和隔离单元的使能,达到分级分层功耗管理的目的,有效降低了空闲状态的各模块动态损耗。

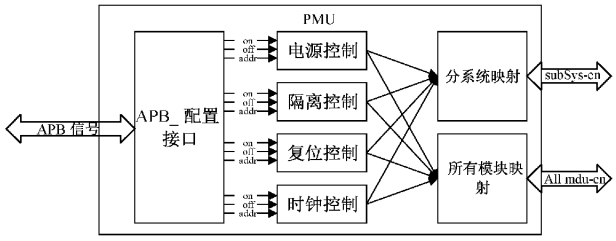

图 9　PMU 功耗管理模块结构

芯片 TOP-UPF 约束布局如图 10 所示,根据各个模块性能需求,在芯片内划分不同的电压域(power domain),插入电源开关控制、隔离器件。

芯片中加密子系统、高速协议子系统以及总线内交换矩阵的功耗较大,对上述模块分别用独立电源域实现(switch-offdomain),SoC 核心子系统采用常开电源域(always-domain),高速协议子系统内根据协议分层,也被

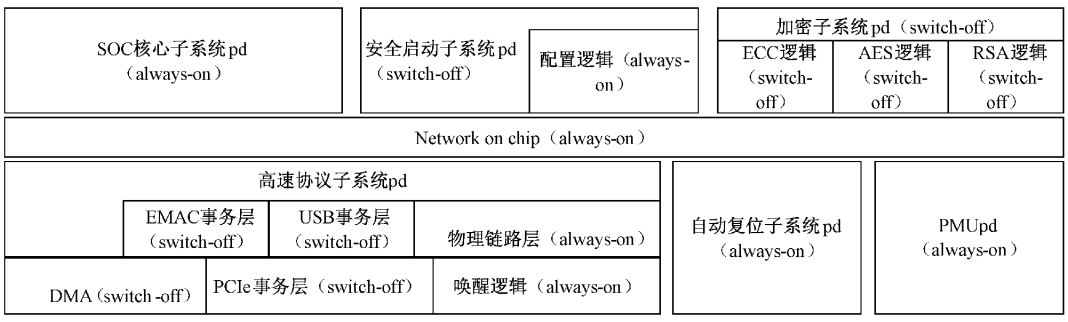

图 10　UPF 约束布局图

分为不同的电压域。设计采用统一标准格式(unified power format,UPF)实现多电压域技术,满足低功耗设计需求。部分约束代码如图 11 所示。

```
#create top power domain
create_power_domain pd_soc_top -include_scope
#create power domain supply
create_supply_port VDD -domain pd_soc_top
create_supply_port VSS  -domain pd_soc_top
create_supply_net VDD  -domain pd_soc_top
create_supply_net VSS   -domain pd_soc_top
connect_supply_net VD  -ports VDD
connect_supply_net VSS -ports VSS
#setting power domain supply
set_domain_supply_net pd_soc_top  -primary_power_net VDD \
-primary_ground_net VSS
#load module upf
load_upf /soc_arm.upf  -scope U_arm_sys
load_upf /security.upf   -scope U_security
load_upf /encry.upf      -scope U_encry
load_upf /high_prot_sys.upf -scope U_protocol
load upf /rst_sys.upf     -scope U_rst_sys
connect_supply_net VDD -ports U_arm_sys/VDD
connect_supply_net VSS  -ports U_arm_sys/VSS
connect_supply_net VDD -ports U_security/VDD
connect_supply_net VSS  -ports U_security/VSS
connect_supply_net VDD -ports U_encry/VDD
connect_supply_net VSS  -ports U_encry/VSS
connect_supply_net VDD -ports U_protocol/VDD
connect_supply_net VSS  -ports U_protocol/VSS
connect_supply_net VDD -ports U_rst_sys/VDD
connect_supply_net VSS  -ports U_rst_sys/VSS
```

图 11　部分 UPF 约束代码

3　芯片测试结果

3.1　芯片接口性能测试

芯片基础性能测试的主要目的是测试数据传输和加解密计算速度,并验证启动时序及各片外接口协议传输的正确性。测试程序,采用 Xilinx PCIE、EMAC、USB 固件驱动设计,软件驱动 AES、ECC 算法。测试结果如表 3、4 所示。

表 3　加密测试结果

模块	数据块	计算时间/ms
AES	64 MB	689
ECC	2 KB	52
RSA	64 MB	600

表 4　高速端口测试结果

模块	版本	传输速率/Mbps
PCIe	Gen2	3 000
EMAC	1 000 Mbps	400
USB	2.0	480

3.2　芯片功耗分析

本设计使用 SYNOPSYS 公司提供的综合工具(design compiler,DC)集成设计环境,进行 RTL 代码综合、实现、功耗分析等工作。通过 VCS 仿真器产生 fsdb 波形文件,将 fsdb 转为 saif 的方法分析功耗。芯片系统功耗如表 5 所示,从功耗报告看出,芯片整体功耗降低到了约 3.5 W,达到设计指标。通过仿真结果及芯片基础性能测试看到,芯片的处理能力没有降低,达到设计预期目标。特定功率单位信息如下,电压单位 1 V,电容单位 1 pf,时间单位 1 ns,动态功耗单位 1 mW,静态功耗单位 1 μW。

表 5　系统功耗表

类别	功耗(优化前)	功耗(优化后)
单元内部功耗(Cell internal power)	2 755	2 202
线路翻转功耗(Net switching power)	1 603	1 259
总动态功耗(Total dynamic power)	3 591	3 496
单元泄漏功耗(Cell Leakage power)	41	34

4　结　　论

本文提出了一种基于高速总线的密码 SoC 设计与实现方案。相较于传统加密方式,采用 SoC 设计理念,实现了高速数据传输存储、直接存储器访问、低功耗的硬件逻辑。设计采用 verilog 语言实现,有多层总线和多协议结构,加密接口、多种高速协议整合,设计 IST-DAT DMA 模块,降低了 CPU 中断和资源消耗,提高了芯片系统整体执行效率;采用多种低功耗设计方法,系统功耗低于 3.5 W。芯片基础性能测试报告分析表明,加密功能及芯片端口传输速率已达到设计要求。多项核心技术使芯片在具备高可靠、高性能的同时,功耗明显降低。在当前自主、可控的芯片大背景下,较先前学者提出的加解密芯片设计方案,在总线利用率、接口传输速率、系统运行效率、系统功耗、芯片迭代成本等方面都有明显优势。

参考文献

[1]　王凯,李伟,陈韬,等. 密码 SoC 中算法 IP 核通用接口模型[J]. 计算机工程与设计,2021,42(10):2799-2807.

[2]　何安平,郭慧波,冯志华,等. 基于异步电路设计的 RSA 算法加密芯片[J]. 计算机工程与设计,2019,40(4):906-913.

[3]　王飞宇,刘剑峰. DPA 攻击中功耗采集技巧研究[J]. 电子技术应用,2015,41(2):123-126.

[4]　何安平,郭慧波,冯志华,等. 基于异步电路设计的 RSA 算法加密芯片[J]. 计算机工程与设计,2019,40(4):906-913.

[5]　简淦杨,蔡田田,习伟,等. 基于异步传输的 IPSEC 安全加密芯片应用[J]. 电子器件,2020,43(2):239-244.

[6]　赵军,曾学文,郭志川. 支持国产密码算法的高速 PCIe 密码卡的设计与实现[J]. 电子与信息学报,2019,41(10):2402-2408.

[7]　颜军,唐芳福,张志国,等. 异构多核人工智能 SoC 芯

片的低功耗设计[J]. 航天控制,2020,38(2):62-68.

[8] 柳泽辰,蒋剑飞,王琴,等. 一种高可靠 SoC 芯片的系统级设计方法[J]. 微电子学与计算机,2018,35(7):54-57.

[9] 闫启政,李斌,沈贵元. 一种基于 AMBA 总线的 SoC 硬件加速器设计[J]. 无线电通信技术,2015,41(1):71-73.

[10] 李涛,张斌,赵冬娥,等. 高速密集数据采集与传输技术研究[J]. 国外电子测量技术,2018,37(3):103-107.

[11] 洪广伟,崔超,虞致国,等. 基于 RISC-V 处理器的 TileLink 与 AXI4 总线桥设计与实现[J]. 微电子学与计算机,2022,39(4):100-108.

[12] SIFIVE I. SiFive tileLink specification [EB/OL]. [2021-12-03]. https://sifive.cdn.prismic.io/sifive/7bef6f5c-ed3a-4712-866a-1a2e0c6b7b13-tilelink-spec-1.8.1.pdf.

[13] COOK H, TERPSTRA W, LEE Y. Diplomatic design patterns, A TileLink case study[EB/OL]. [2021-07-20]. https://carrv.github.io/2017/papers/cook-diplomacy-carrv2017.pdf.

[14] MCMILLAN K. Modular specification and verification of a cache-coherent interface [C]. 2016 Formal Methods in Computer-Aided Designs (FMCAD), MountainView, CA, USA: IEEE Press, 2016: 109-116.

[15] 陈琳,严迎建,周超,等. ECC 处理器时间随机化抗 DPA 攻击设计[J]. 电子技术应用,2015,41(10):103-106.

[16] 黄泽林,乔树山,袁甲. 物联网节点 SoC 的功耗管理器设计[J]. 微电子学与计算机,2017,34(10):1-4,10.

[17] 钟杨源,朱宇耀,施隆照. 基于 SOC 的低功耗管理模块设计[J]. 中国集成电路,2016,25(4):38-42.

[18] 朱佳琪,陈岚,王海永. 一种低功耗时钟树的设计和优化方法[J]. 微电子学与计算机,2021,38(10):85-90.

作者简介

王凯,硕士研究生,主要研究方向为集成电路设计、IC 验证技术。

E-mail:745579593@qq.com

曲英杰,博士,教授,硕士生导师,主要研究方向为集成电路设计与数据加解密。