吴万强

数字芯片设计工程师

# 基本信息

电 话：13438337364

邮 箱：wanqiangwu@qq.com

现居城市：成都

出生年月：1995-07

政治面貌：中共党员

# 教育背景

西南民族大学， 电子与通信工程硕士， 2021年7月

郑州工业应用技术学院， 通信工程学士， 2018年6月

# 专业技能

* 熟练使用Verilog HDL进行RTL开发
* 熟悉SystemVerilog、C编程
* 熟练使用VCS、Verdi、Spyglass等EDA工具
* 熟练使用DC、Formal等工具进行PPA分析和一致性检查
* 熟练使用CLP Check、PTPx、PowerPro等工具进行UPF检查和功耗分析
* 熟练使用Python\Shell编写脚本
* 熟悉EMU仿真使用

# 工作经历

成都忆芯科技有限公司，数字电路设计高级工程师，2021年7月至今

* 根据需求设计模块整体框架，完成模块级LLD设计文档
* 根据LLD实现高质量的RTL，并进行Lint、CDC、DC时序分析等代码质量检查
* 负责两个子系统Harden Block的集成，及SDC、UPF撰写
* 完成Harden Block SDC Check、UPF CLP Check、Netlist Formal 一致性检查
* 完成芯片所有模块的Power统计
* 完成Memory自动生成系统开发、测试

# 项目经验

## 12nm PCIe Gen4 SSD主控芯片，2021年7月至2022年5月

### 1. AXI\_Lite2APB\_bridge设计

**模块功能**：该模块实现AXI\_Lite协议转换为APB协议；

**负责内容**：从学习AXI\_Lite及APB协议开始，了解每个协议的接口时序，构思两种接口协议对接数据传输桥接方案，绘制AXI\_Lite2APB Bridge 模块LLD框图(从系统至细节的4级框图)，邀请同事设计方案进行Review，根据Review结果修改设计方案，之后根据设计框图撰写模块文档；

### 2. Security算法模块学习、维护与Freeze收尾工作

**模块功能**：

**SM2\RSA**：这两个模块作为国密及商密签名、验签的核心算法支持模块，国密方面实现了椭圆曲线底层模加、模减、模乘、模逆、蒙哥马利模乘、点加、点乘、点倍等底层算子可以灵活支持SM2算法协议层实现；商密方面实现了模加、模减、模乘、模幂、蒙哥马利模乘、模逆、模除等底层算子可以灵活支持RSA算法协议层实现；

**SM3\SHA256**：这两个模块实现国密及商密哈希算法，主要为了支持签名验签或者可信计算过程中信息摘要的生成；这两种摘要算法在算法结构上面较为相似，只是初始向量不同，因此可以采用相同的架构实现；

**SM4\AES256**：这两个模块实现国密及商密的对称加解密算法，支持SSD主控芯片在数据通路读写过程中实时进行加解密保证用户数据的安全性；这两个模块均支持ECB、CBC、XTS三种加解密模式；并支持多组密钥，以及密钥切换功能；支持密钥二级加密，可以提供更高的数据安全性；

**负责内容**：

进入项目组时以上模块功能稳定，没有新的开发需求，主要负责学习模块SPEC及RTL，补充完善SPEC，以及最后各个模块覆盖率检查；

## 8nm PCIE Gen5 SSD主控芯片MPW，2022年5月至2023年11月

### 1. 负责Security性能提升及国密二级修改，提升芯片安全性

**模块功能**：前代芯片按照国密一级安全要求进行设计，而此代芯片需要进行安全性升级，以满足国密二级安全要求，国密二级相对于国密一级主要是在抵御侧信道攻击方面要求的提升；另外芯片要支持PCIe Gen5实时数据加解密的性能，因此对于模块性能也需要进行翻倍提升；

**负责内容**：

**SM2国密二级修改**：学习SM2的侧信道攻击原理，梳理防御侧信道攻击的方法，总结适合当前SM2模块的防御方案，修改设计方案并进行Review；主要采取了隐藏标量乘功耗轨迹图以及随机化功耗信息的方式，对SM2进行了修改，实现了满足国密二级的安全性提升。

**SM4国密二级修改及性能提升**：学习SM4的侧信道攻击原理，梳理防御侧信道攻击的方法，总结适合当前SM4模块的防御方案，修改设计方案并进行Review；主要采取算法级掩码方案，通过布尔掩码的方式，掩盖其非线性变换的功耗信息，实现了满足国密二级的安全性提升；该侧信道防护方案申请了一项专利。在性能提升方面，受限于算法分组要求，采用了双加解密核心架构，使得数据处理性能翻倍；而在XTS模式下，存在密文窃取的过程会打断数据流水，针对这个去采用了拼流水、Buffer缓存的方式将密文窃取的多个Cycle节省出来，提高了数据总线的利用率，从而实现翻倍后14GB\s的实时数据加解密性能；该性能提升方案申请了两项专利；

**HASH模块独立及性能提升**：

前代芯片HASH计算模块集成在其他模块内，存在较多耦合设计，不利于修改；现在将其独立出来放在TOP上，模块对接自研消息总线收发CMD及CPL，对接AXI总线，作为Master进行数据读取；针对性能做了提升，增加少量Buffer，提前缓存分组数据，减少数据输入延时，提升整体性能；由于SHA1、SHA2协议族中的多个HASH算法存在相似的结构，用少量分支结构实现了多种HASH算法的支持；将以512Bit分组处理的SM3、SHA256、SHA1、SHA224几种算法集成到一个模块实现，将以1024Bit分组处理的SHA384、SHA512、SHA512\_256、SHA512\_384几种算法集成到一个模块实现，将原来支持2种摘要算法，提高到支持8种摘要算法。采用多核心并行的方式，使得HASH模块整体数据处理性能从之前的几百兆提升至14GB\s。

### 2. 负责两个Harden Block集成与交付

**负责内容**：

将两个Harden Block的RTL进行集成，使用Spyglass对Block进行Lint检查、CDC检查，撰写SDC及UPF，对Block进行DC综合，评估Block的面积大小及时序情况；使用PowerPro对模块进行CG率检查，并根据报告修改设计，保证负责模块的CG在90%以上；在整个项目的各个阶段完成RTL、Post DFT Netlist、PG Netlist 的 CLP Check，以及RTL2Gate、Gate2Gate的FM Check；

### 3. 芯片各模块Power统计

**负责内容**：

收集各个Harden Block在IDLE、读、写等场景下的波形，对波形进行处理，截取成每个场景下的特定波形，不包含其他场景的波形，并将处理好的波形转换成SAIF类型的波形文件；配合后端提供的各个Harden Block的PT Session，使用PTPx工具对各个Harden Block的各个工作场景进行平均功耗分析，并将各个场景的数据汇总成Excel表格。

## 8nm PCIE Gen5 SSD主控芯片Full Mask，2023年11月至今

### 1. 负责两个Harden Block集成与交付

**负责内容**：

将两个Harden Block的RTL进行集成，使用Spyglass对Block进行Lint检查、CDC检查，撰写SDC及UPF，对Block进行DC综合，评估Block的面积大小及时序情况；使用PowerPro对模块进行CG率检查，并根据报告修改设计，保证负责模块的CG在90%以上；在整个项目的各个阶段完成RTL、Post DFT Netlist、PG Netlist 的 CLP Check，以及RTL2Gate、Gate2Gate的FM Check；

### 2. Memory生成及生成、测试Flow升级修改：

**模块功能**：设计采用了通用的Memory模块，为使用者提供了统一的接口，在内部实现SP、TP、TPS等各种Memory的连接；由于Memory修改频繁，有很多工作可以进行系统化的脚步生成，我们开发了Memory自动生成系统；在Memory生成之后对所有的Memory进行本地测试，测试通过后Release给到需求方使用。

**负责内容**：

**Memory生成**：基于现有Memory TCL生成脚本进行修改以避免除了深度、宽度以外更细致的需求导致的无法进行区分的问题，主要在命名规则上进行更新；

**Memory自动生成系统**：使用Python、TCL配合开发了Memory自动生成系统，根据用户的Memory需求，输入到Memory自动生成系统中，系统会自动以满足Min Period 及 面积最优为目标，进行多轮自动评估、自动拆分，最终遍历所有满足用户需求的Memory方案，并其中输出面积最小的方案给到用户；并将最终的方案转换成对应的Verilog文件。在这个系统中，我主要负责Memory自动拆分方案设计、实现，以及Memory自动生成系统集成、测试及验证。

**Memory本地测试方案增强**：之前的Memory测试方案较为简单，仅将地址作为数据依次写入对应地址中，这就导致Memory高Bit位没有被测试覆盖；现在按照Memory宽度进行数据全随机输入，如果Memory有Bit Enable的功能，针对每一个可以Mask的Bit控制位也进行全随机Disable；对于有ECC需求的Memory，还加入了ECC功能验证，主要手段是在Memory每个地址都写入数据后，在UCLI模式下利用TCL脚本随机强制修改每个Memor块中的一些数据bit，最后在读取数据后判断ECC是否生效。

# 专利

SM4-XTS性能提升

AES-XTS性能提升

SM4侧信道防护

# 在校期间科研成果

[1] 吴万强, 彭良福, 甘桂, 王逸凡. 基于SOPC的实验室负荷智能监测装置[J]. 实验室研究与探索, 2020,39(6):78-82,107．

[2] Wanqiang Wu, Liangfu Peng, Gui Gan. Oven Controlled Crystal Oscillator Control Based on BP Neural Network Tuning PID[J]. Frontiers in Signal Processing, 2020, 4(1):22-29.

[3] 甘桂, 彭良福, 吴万强. 基于GPS驯服晶振的高精度频差测量[J]. 电子世界, 2019(14): 82-83.

# 自我评价

学习能力强，对新事物保有好奇心，能快速适应新环境；良好的沟通和团队合作能力；能与他人合作，共同完成目标；遇到困难总是相信有办法解决。