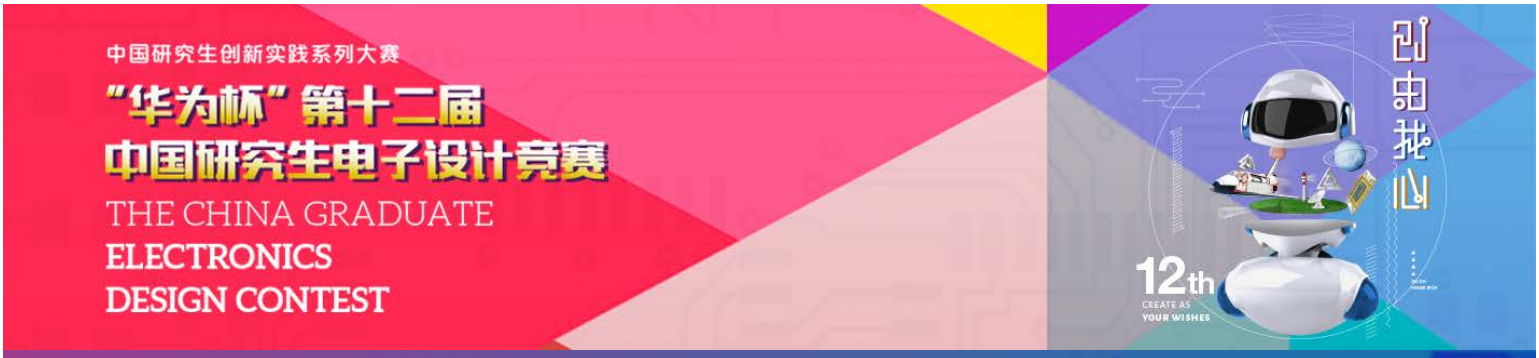


参赛说明
命题说明
文件下载

命题说明

华为命题

赛题一:逻辑实现AES\DES\SM4\SM1加解密算法的SPA和DPA防攻击设计。

描述及要求：

1.逻辑实现一个AES\DES\SM4\SM1加解密算法设计（选择任意一个即可）。具备防止各种已知SPA\DPA\DFA（二阶或者高阶）攻击的能力。 ECB\CBC\CTR\XTS等模式不限，选择一种多种均可。SBOX采用实时计算方式实现，需要引擎全通路加掩。

2.理论分析SPA\DPA（二阶或者高阶）攻击对AES\DES\SM4\SM1（加入防攻击功能）的理论破解时间。

3.时钟频率不限，资源和功耗不能过大。可采用全硬件实现，也可采用软硬件结合。

评审得分点:

1.AES\DES\SM4\SM1具备防止各种已知SPA\DPA（二阶或者高阶）攻击的能力，没有任何防护漏洞。

2.SPA\DPA防攻击理论清晰，理论破解时间越长得分越高。

输出要求：

1.算法设计文档和算法代码。

2.详细设计文档和逻辑代码，或软件代码。

赛题二:采用软硬件结合的方式实现ECC\RSA\SM2\SM9（四选一即可）算法(要求具备防DFA\SPA\DPA能力)。

描述及要求：

1. ECC\RSA\SM2\SM9需要的模幂、点乘、模逆、模乘、模加、逻辑加、逻辑减、算术乘、算术除等模运算、逻辑运算、算术运算使用硬件实现。其他高 层算法可采用软件实现。（RSA密钥长度至

少2048位，ECC\SM2\SM9密钥长度256位，采用素域实现）。模幂要求为非CRT模幂。具备防止各种已知SPA\DPA\DFA（二阶或者高阶）攻击的能力。

2.可只实现点乘或模幂运算，其它高层算法不强制要求。

3.点乘、模幂至少可以达到25次/S（对应时钟频率为120MHz，其他时钟频率可等比例折算）。

评审得分点:

1.防攻击能力越强越全面，没有任何防护漏洞。得分越高。

2.RSA密钥位宽至少为2048位，位数越长，得分越高。

3.ECC\SM2\SM9密钥位宽至少为256位，位数越长，得分越高。

4.性能越高，得分越高。

输出要求：

1.算法设计文档和算法代码。

2.详细设计文档和逻辑代码、软件代码。

赛题三:硬件实现真随机\伪随机数生成。

描述及要求：

1.对随机源及随机数的随机性建立模型进行分析。需要分析安全性、复杂度、软硬件实现效率。

2.随机数后处理时钟频率120M。

3.采用全数字方式实现。

4.对随机数进行测试。能通过NIST SP-800、AIS31等检测标准。

评审得分点:

1. 随机源及随机数的随机性模型完整、详尽。

2. 逻辑规模越小，得分越高。

3. 产生的数据随机性越好，能通过NIST SP-800、AIS31等检测标准，得分越高。

4. 随机数生成算法的安全性越高，无被攻击的安全漏洞，得分越高。

输出要求：

1. 算法设计文档和算法代码。

2.详细设计文档和逻辑代码、或软件代码。

赛题四：逻辑实现ZUC算法的SPA和DPA设计。

描述及要求：

1.逻辑实现一个完整的ZUC算法设计。具备防止各种已知SPA\DPA（二阶或者高阶）攻击的能力。防护手段不限。

2.理论分析SPA\DPA（二阶或者高阶）攻击对ZUC的理论破解时间。

3.时钟频率不限，资源不限，功耗不限。采用VHDL\VERILOG实现。

评审得分点:

1.具备防止各种已知SPA\DPA（二阶或者高阶）攻击的能力，无安全漏洞。

2.SPA\DPA防攻击理论清晰，理论破解时间越长得分越高。

输出要求：

1.算法设计文档和算法代码。

2.详细设计文档和逻辑代码。

赛题五：多核一致性的拓扑结构设计

描述：

多核一致性一直是处理器领域的研究热点，如何提高一致性系统数据访问的效率及便于扩容是其中的技术关键点。这些性能取决于一致性方案及对应的拓扑结构。

要求：

设计一种多核一致性的拓扑结构（不限制具体的CPU类型及一致性协议），使以下重要指标最优：

1.系统数据吞吐率及延时

2.对应的实现逻辑的面积

3.是否利于高速电路实现

是否利于CPU核的增减

作品格式：

1.输出设计文档，给出关键数据

2.给出对应参考设计代码及仿真、实现的结果

评审标准：

1.方案的正确性、新颖性、实用性和可实现性

2.关键数据的完备性、正确性

3.参考设计正确性

赛题六：组建HIFI音频随身播放器

描述：使用已有或者自主设计的播放主板，不限制方案和芯片类型，要具备耳放功能，要求电池供电，体积不能太大，可以随身携带

要求：

1：支持32bit/192K接口

2：支持耳放功能

3：支持高阻抗耳机

4：高信噪比，高动态和高立体分离度

5：电池供电，体积小，可以随身携带

加分项：

1：支持DSD硬解码

2：体积越小越好

作品格式：

1、测试视频

2、设计方案文档

3、提供整机

评选标准：

1：信噪比SNR越高越好，THD+N越低越好

2、在满足要求下，成本低，体积小者优胜

3、在满足要求下，音频指标好者，体积小者优胜

赛题七：运动状态（乒乓球/羽毛球）识别及分析

命题描述：

乒乓球/羽毛球运动中运动状态的识别分析。

要求：

1、设计腕带类电子设备，在乒乓球/羽毛球运动中佩戴于持球拍手位，辅助实现运动状态检测分析，呈现分析结果。

2、平台方案不限，交互方式不限，终端侧成品可佩戴于手腕；

评审标准：

1、进入单项球类运动（乒乓球/羽毛球）模式，在运动过程中实时检测分析挥臂/接球次数、平均挥臂速度、过程中步数、跳击、捡球次数等运动指标，对应能检测出的动作种类（可自行挖掘运动特征）越多越好，检测结果越准确越好；（60%权重）

2、扩展项——支持在两种运动开始后5min内自动检测出运动类型；（10%权重）

3、扩展项——设备间支持三人组网及标识识别，裁判位可录入分数，选手位可根据分数录入情况判定发球方；（10%权重）

3、扩展项——可以按照泛命题来做设计，比如通过神经网络算法实现运动的自学习自校准达到越用越准的效果、运动分析的超低功耗实现等，在该命题内自由发挥的同时自行挖掘设计亮点；（20%权重）

4、加分项——如选用MCU平台，移植并基于华为LiteOS开源嵌入式操作系统（华为开发者社区有详细的移植操作指导等）完成开发可加分。

作品格式：

1、演示样机；

2、算法设计文档和算法代码；

3、详细软硬件设计文档（包括原理图、PCB）

赛题八：实现一个Sparse Matrix-Multiply-Vector Accelerator

命题描述：

实现一个Sparse Matrix-Multiply-Vector (SpMV) Accelerator，提供RTLcode，加速算法，并演示计算流程。我们提供下列矩阵集合（包含MATLAB mat-file格式，Matrix Market 格式，和Rutherford/Boeing格式，做题时选其中一种格式即可）：

http://www.cise.ufl.edu/research/sparse/matrices/HB/beause.html

http://www.cise.ufl.edu/research/sparse/matrices/Bai/rbsa480.html

http://www.cise.ufl.edu/research/sparse/matrices/Bai/qc2534.html

http://www.cise.ufl.edu/research/sparse/matrices/DRIVCAV/cavity07.html

http://www.cise.ufl.edu/research/sparse/matrices/Fluorem/GT01R.html

http://www.cise.ufl.edu/research/sparse/matrices/HB/arc130.html

http://www.cise.ufl.edu/research/sparse/matrices/HB/bp_1600.html

http://www.cise.ufl.edu/research/sparse/matrices/HB/mbeause.html

http://www.cise.ufl.edu/research/sparse/matrices/Hollinger/g7jac010.html

http://www.cise.ufl.edu/research/sparse/matrices/JGD_Homology/ch6-6-b3.html

http://www.cise.ufl.edu/research/sparse/matrices/JGD_Homology/n2c6-b4.html

http://www.cise.ufl.edu/research/sparse/matrices/JGD_GL7d/GL7d11.html

请自行下载矩阵，并将其转换为32-bit浮点。以Dense或者CSR/COO/HYB等常见稀疏矩阵存储格式(或者自定义的某种稀疏存储格式)，将上面所列12个矩阵分次存入内存空间。利用所提供的脚本生成与这些矩阵（Mi x Ni）尺寸相配的随机向量（N x 1）并存入内存。向量和矩阵的存入不计入运算时间。

所设计的加速器，需要从内存中读取矩阵和向量，并传入加速器内部实现矩阵和向量相乘，并最后将结果存入内存。

实现要求：

1.所有矩阵，向量元素均为single-precision floating point（32 bits）长度

2.加速器的硬件逻辑中最多存在256个fp32浮点乘法器

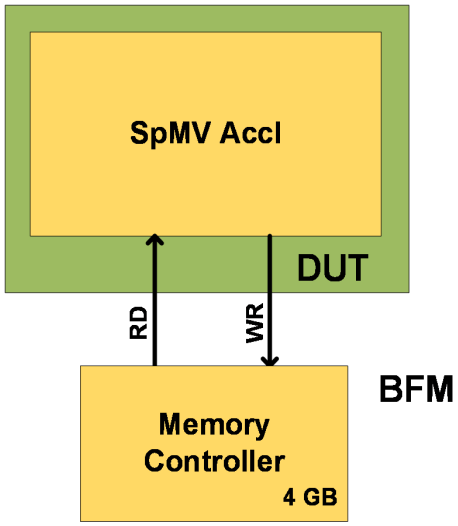
3.12个矩阵的格式预处理可由软件处理；但对随机产生的12个向量的预处理必须由加速器的硬件逻辑完成。

4.允许将附加和预处理后得到的信息存入内存

5.不允许用有损的方式

6.加速器与内存之间的读、写的数据位宽各为128-bit。为简化非关键特性，内存频率和加速器同频，接口为Dual Port SRAM，单cycle延迟。（见图1）

7.由脚本随机产生的向量也会有一定程度的稀疏率（30%~80%）。参赛者可以结合稀疏向量一同加速。（注意不能对向量预处理。注意处理向量的硬件代价）



评审得分点：

1.计算结果要正确，可忽略32bit精度结果的误差

2.所费的运算时间越少，得分越高

3.通常，如果矩阵不做任何稀疏存储，仅以Dense格式进行运算，则运算时间肯定会比稀疏化后矩阵的时间长；如果根据CSR/COO/HYB (或者自定义的某种稀疏存储格式)稀疏存储，并采取与此有关的优化手段(跳0等)，则运算时间可以大为降低；

4.逻辑规模越小，得分越高

5.加速器对内存访问带宽越小，得分越高

6.功耗越小，得分越高

输出要求：

1.详细的算法解释文档，和算法代码。请在文档中写明加速亮点。

2.详细的设计文档，和RTL代码（Verilog）。请在文档中写明低功耗设计点。

3.硬件对上述12个benchmarks的加速性能分析文档。

4.演示环境

奖励办法：

一等奖4名，10000元/队

二等奖10名，5000元/队

英特尔命题

命题描述：

基于英特尔公司的FPGA产品或开发板。自主设计，独立完成基于深度学习，嵌入式视觉，自动驾驶，人工智能等应用特别是能够采用OpenCL工具且具备一定功能的应用系统或作品。

评审标准：

设计阶段 Design Phase	评分标准 Category	得分 Score
设计概念 Design Concept	复杂性 Complexity	10
	功能性 Functionality	20
	创新性 Innovation	10
设计的实现 Design Implementation	完整性 Completeness	40
文稿 Documentation	完整性 Completeness	20

奖励办法：

一等奖1名，奖品为苹果电脑

二等奖2名，奖品为价值3000元奖品

三等奖3名，奖品为价值为2000元奖品