**2020年新工科联盟-Xilinx暑期学校团队项目设计文档**

**设计文稿提交格式**

**(Project Paper Submission Template)**

|  |  |
| --- | --- |
| **作品名称** | HLS实现的AES-128简单加解密引擎 |
| **板卡型号** | PYNQ-Z2 |
| **所在班级** | B-10 |
| **成员姓名、学号、学校** | 胡鹏 ——20BO036A——中科院计算所  张聪武 ——20BO037A——中科院计算所 |
| **Github链接** | [*https://github.com/zhbeiluo/xlnx-aes-project*](https://github.com/zhbeiluo/xlnx-aes-project) |

**第一部分**

设计概述 /Design Introduction

（1.请概括地描述一下你的设计，可包括本设计目的、学习到的知识点、应用方向或者设想的应用场景等；2. 经组内成员讨论后以表格的形式描述项目中各成员在项目中发挥的作用或者贡献百分比；3.作品的展示照片）

1. 设计描述
2. 目的

高级加密标准（AES）是美国国家标准技术研究所（NIST）在2001年发布的一个对称分组密码算法，旨在取代DES成为广泛使用的标准。

AES的明文分组的长度为128位，即16字节，密钥长度可以为16字节，24字节或32字节（128位、192位或256位）。根据密钥的长度，算法被称为AES-128，AES-192或AES-256。本实现中我们采用的是AES-128。

本设计的目的主要是针对大文件的加解密，AES-128一次处理128位显然不够。因此，我们采用了AES五种工作模式里的CBC（cipher block chaining，密文分组链接模式），CBC模式是非常常用的工作模式，特别适合大文件的加解密。

1. 知识点

本设计涉及到的知识点主要有：AES-128算法、AES的CBC工作模式、Vivado HLS语法等。

1. 应用场景

本设计提供了AES-128的加解密操作的一个demo，设计的应用场景主要是提供给用户快速搭建AES加解密的FPGA原型所需的IP，帮助用户快速实现设计。

1. 组员作用

|  |  |  |
| --- | --- | --- |
| 组员 | 主要作用 | 贡献度 |
| 胡鹏 | AES-128算法的HLS实现，立项文档，设计文档 | 50% |
| 张聪武 | AES-128算法的调试，设计文档 | 50% |

3、作品展示

我们在Vivado HLS工具中对AES-128设计进行了模拟测试，测试结果如下。可见加解密前后数据是一致的，说明我们AES-128的算法IP的功能是正确的。

图片包含 游戏机, 截图

描述已自动生成

**第二部分**

系统组成及功能说明 /System Construction & Function Description

（请对作品的1. 计划实现及已实现的功能；2. 项目系统框图；3. 使用的技术方向做说明）

1. 已实现的功能

我们用HLS实现了AES-128算法，并进行了仿真测试，测试表明我们的AES-128算法实现的功能正确。

1. 项目系统框图

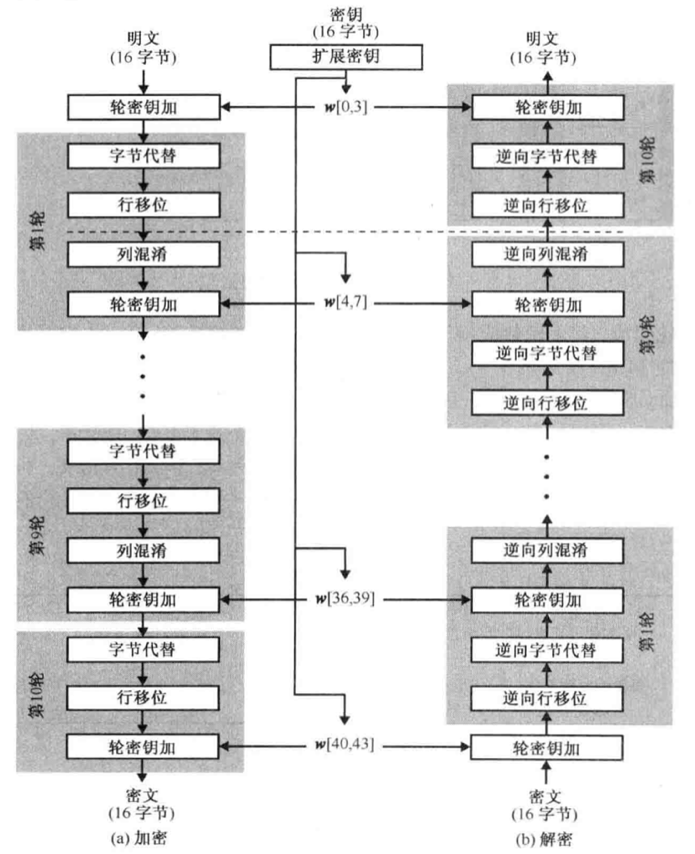
系统的Block Design的结构框图如下，其实aes\_0就是我们用Vivado HLS工具导出的AES-128算法的IP。

图片包含 游戏机, 截图

描述已自动生成

1. 使用的技术
2. 基础加密算子：AES-128

AES算法的主要步骤有：轮密钥加：AddRoundKey，字节替代：ByteSub，行移位： ShiftRow，列混肴： MixColumns，如下图：



1. 工作模式采用：CBC模式

AES的密文分组链接（CBC）工作模式的主要特点如下：

①加密算法的输入是当前明文分组和上一次密文分组的异或，因此加密算法的输入不会显示出与这次的明文分组之间的固定关系，所以重复的明文分组不会在密文中暴露出这种重复关系。因此可以加密长度大于分组长度的消息。

②使用相同的密钥。

③如果最后的分组不完整需要padding。

密文分组链接（CBC）模式的加解密流程图如下：

**图片包含 游戏机, 钟表

描述已自动生成**

**第三部分**

完成情况及性能参数 /Final Design & Performance Parameters

（作品已实现的功能及性能指标）

1. 已实现的功能

如第一部分的第三点所示，我们在Vivado HLS工具中对AES-128设计进行了模拟测试，测试结果显示加解密前后数据是一致的，说明我们AES-128的算法IP的功能是正确的。

2、性能指标

Solution1是不进行任何优化的方案，solution2是对关键数组进行array\_partition优化，主要循环增加了流水线优化。性能对比如下，solution2的延迟大大降低了，但是资源开销也增大了，尤其是LUT的使用增加了很多。

图片包含 游戏机, 橱柜

描述已自动生成

图片包含 游戏机, 截图

描述已自动生成

**第四部分**

总结 /Conclusions

（谈一谈完成暑期学校课程后的收获与感想。请每位组员分开写。）

1. 胡鹏的感想

首先感谢Xilinx开展的暑期学校项目，以及授课老师和助教的这两周的辛勤付出。

在这两周里我学习了Vivado HLS的使用，这对于本科学习软件工程，没有一点硬件基础的我来说，HLS能帮助我快速实现原型设计，HLS提供的directive优化能非常快速地实现包括流水线、循环展开等优化。相信这些知识能帮助我后续的学习和工作。