1.简易数据传输加密处理电路

设计一个简易的数据传输加密处理电路，包括数据源生成电路、密码流生成电路、数据加密电路、数据传输电路、数据解密电路（测试验证用），题目包含基本要求和发挥部分。题目不涉及实体硬件电路，所有功能的设计及仿真均在EDA开发环境中实现，竞赛根据总体设计框图及说明、各个模块电路设计说明、时序说明、仿真结果、资源报告、设计总结和程序源代码评定成绩。

1. **任务**

设计一个简易数据传输加密处理电路，实现对数据源数据进行加密并将密文数据进行串行传输；同时设计一个数据接收及解密电路，将密文数据解密成明文数据并存储在RAM中，用来验证加解密电路。

简易数据传输加密处理电路的系统框图如图1所示。待加密的数据由**数据源生成电路**产生，V1为待加密数据；密钥数据由**伪随机序列生成电路**产生，V2为密钥数据流；**数据加密及传输电路**将V1和V2进行加密生成密文数据，并将密文数据V3串行输出；**数据接收及解密电路**将接收到的密文数据V3与解密数据流V4进行解密运算得到明文数据V5，随即将明文数据V5存入RAM中。



图1 简易数据传输加密处理电路的系统框图

1. **要求**
2. **基本要求**
3. 设计一个数据源生成电路：
4. 待加密数据V1由数据源生成电路产生，电路需设计必要的输入、输出控制信号和数据输出接口；
5. 数据源输出的待加密数据V1为4bit宽度的并行数据；
6. 每次使能信号到来，数据源生成电路将依次输出从0到15的二进制数据（共计16个4bit数据），每次时钟的上升沿将数据推出，时序图如图2所示。



图2 数据源生成电路时序图

1. 设计一个伪随机序列生成电路用来产生加密和解密的密钥数据：
2. 密钥数据流V2由伪随机序列生成电路产生，电路需设计必要的输入、输出控制信号和数据输出接口；
3. 密钥数据流V2为1bit的串行数据；
4. 密钥数据流V2为的m序列，设其初始状态为（a4，a3，a2，a1，a0）=（1，0，1，0，1），每次时钟的上升沿将数据推出。
5. 设计数据加密及传输电路：
6. 数据加密及传输电路需设计必要的输入、输出控制信号和数据输入、输出接口；
7. 电路将V1的并行数据和V2的串行数据进行加密运算，并将加密后的密文数据V3以串行发送方式传输；
8. 传输协议可使用常用的串行传输协议，也可根据题目要求使用自定义串行传输协议。
9. 设计数据接收及解密电路：
10. 数据接收及解密电路需设计必要的输入、输出控制信号和数据输入、输出接口；
11. 电路根据串行传输协议接收密文数据V3，并将V3和V4进行解密运算，解密出的明文数据V5为4bit宽度的并行数据；（注：由于解密过程为加密过程的逆过程，因此密钥数据流可直接调用加密过程中的伪随机序列生成电路来生成V4）
12. 为验证解密数据，电路需将明文数据写入RAM中。RAM可不用设计，但解密电路需产生写入RAM的控制信号，控制信号如图3所示。



图3 RAM写入时序图

1. **发挥部分**



图4 简易数据传输加密处理电路的系统框图（发挥部分）

1. 要求数据加密及传输电路增加参数配置接口（如图4所示）：
2. 参数配置接口为4bit输入数据，配置数据可由用户给定；
3. 参数配置数据即为m序列的初始状态值，数据加密及传输电路可根据参数配置数据V6配置伪随机序列生成电路，使其根据不同的初始状态值产生不同的密钥数据流；
4. V3的密文数据需加入参数配置头（配置头格式自定义），以备数据接收及解密电路解析出配置参数的数值。
5. 要求数据接收及解密电路增加参数配置解析功能：
6. 由于V3密文数据中加入了参数配置头，电路需正确解析出配置参数V6，并将V6值配置给伪随机序列生成电路，才能产生与加密密钥相同的V4密钥数据流。
7. **说明**
8. **题目相关的必要说明**

用Quartus II建立工程时，选择Cyclone II系列的EP2C35F672C6作为目标器件；硬件描述语言使用VHDL或Verilog均可，并在关键代码部分需进行注释。

1. **m序列简介**

m序列是最长线性反馈移位寄存器序列的简称。它是由线性反馈的移位寄存器产生的周期最长的序列。以一个4级线性反馈移位寄存器为例给出一个m序列的例子。设其初始状态为（a3，a2，a1，a0）=（1，0，0，0），则在移位一次时，由a3和a0模2相加产生新的输入a4=1⊕0=1，新的状态变为（a4，a3，a2，a1）=（1，1，0，0）。这样移位15次后又回到初始状态（1，0，0，0）。产生的m序列如图5所示。

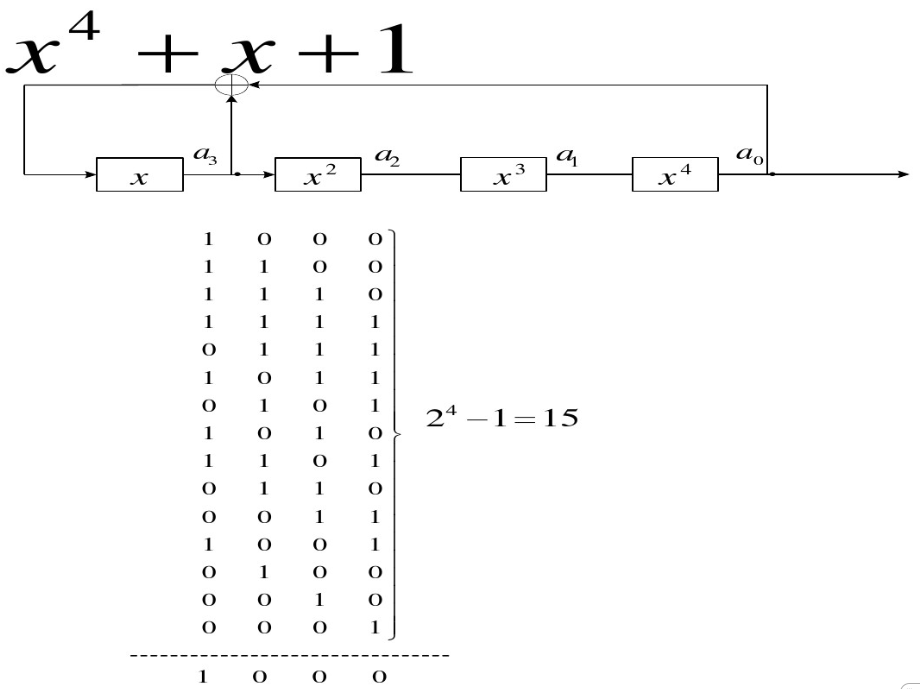


图5 m序列的产生

1. **加密解密原理简介**

根据异或运算的可逆性，对任意的两串二进制数做异或运算，得到的结果再与其中任意一串二进制数做异或运算，之后将得到另一串二进制数。即a ⊕ b = c，则b ⊕ c = a（a，b，c分别表示一串二进制数）。那么，若a是想要加密的信息，则有一密钥b，对a和b做异或运算，得到的c就是加密后的信息，可进行传输。得到c后，只需要再与b做异或运算，即可得到原信息a。若应用到字符串上，则字符串上每一个字符都表示一串二进制数。

1. **评分标准**

|  |  |  |  |
| --- | --- | --- | --- |
| 设计报告 | 项目 | 主要内容 | 分值 |
| 系统方案 | 方案选择、论证 | 4 |
| 理论分析与计算 | 进行必要的分析、计算 | 4 |
| 电路与程序设计 | 电路设计  程序设计 | 4 |
| 测试方案与测试结果 | 表明测试方案和测试结果 | 4 |
| 设计报告结构及规范性 | 表格的规范性 | 4 |
| 小计 |  | **20** |
| 基本要求 | 完成第（1）项目 | | 10 |
| 完成第（2）项目 | | 10 |
| 完成第（3）项目 | | 25 |
| 完成第（4）项目 | | 15 |
| 小计 | | **60** |
| 发挥部分 | 完成第（1）项目 | | 10 |
| 完成第（2）项目 | | 10 |
| 小计 | | **20** |
| 总分 | | | **100** |

**设计报告内容：**

1. 设计思路概述；
2. 总体设计框图及详细说明；
3. 时序说明；
4. 模块设计框图、引脚说明、相关时序；
5. 代码及必要注释；
6. 仿真结果：对顶层电路及中间信号的仿真时序图进行必要的截图，并做必要的说明；对顶层电路的综合结果进行截图；
7. 结论；
8. 其它需要说明的内容。