

基于 FPGA 的高速国密 SM4 光纤通信系统方案

黄沛昱, 宋佳波, 贾洋凡

(重庆邮电大学光电工程学院, 重庆 400065)

摘要: 随着光纤通信技术在工业物联网中的广泛应用, 越来越多的密码算法被应用到物联网嵌入式设备中来保障数据传输的安全性。其中, SM4 分组密码算法是我国自主研发的商用密码算法, 应用于无线局域网和物联网数据加密。嵌入式设备在光纤保密通信中对加解密速度要求很高, 通过软件进行加解密的速度较慢, 满足不了实时性高的应用场景。因此, 基于现场可编程门阵列(FPGA, field programmable gate array)和 SM4 算法, 设计了实时性高、安全性强的光纤通信系统。通过 FPGA 实现 SM4 算法加解密以及数据传输的介质访问控制(MAC, medium access control)层接口处理, 提出 SM4 算法硬件实现架构的优化方案, 采用流水线的方式缩短关键路径, 提高系统时钟频率, 并通过 S 盒变换并行处理加快数据的替换操作, 结合双缓存的处理方式, 减小数据读取时延, 使缓存区数据处理更加容易, 丢包率大大减小, 所提方案极大地提高了系统数据的吞吐量。实验结果表明, 所提方案的 SM4 算法加解密模块与同类型设计相比, 在资源消耗相差不大的情况下吞吐量更大, 可达 25.6 Gbit/s, 受限于万兆 SFP+光模块, 整个光纤通信系统吞吐量最高为 9.4 Gbit/s, 对于 128 bit 数据加密平均耗时为 0.47 μ s, 解密平均耗时为 0.28 μ s, 可应用于多种物联网保密通信场景。

关键词: 光纤通信; FPGA; 数据加密; SM4; 流水线

中图分类号: TN918

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023082

High speed national secret SM4 optical fiber communication system scheme based on FPGA

HUANG Peiyu, SONG Jiabo, JIA Yangfan

School of Opto-electronic Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: With the increasing use of optical fiber communication technology in the Industrial Internet of Things, cryptographic algorithms play a crucial role in ensuring the security of data transmission in embedded device environments. The SM4 packet cipher algorithm, developed independently in our country, is widely applied to wireless LAN and Internet of Things data encryption. However, the software-based encryption and decryption

收稿日期: 2023-04-06; 修回日期: 2023-07-26

通信作者: 宋佳波, songjb1219@163.com

基金项目: 国家自然科学基金(61801061); 中国高校产学研创新基金(2021BCA02004)

Foundation Items: The National Natural Science Foundation of China (61801061), Industry-University-Research Innovation Fund for Chinese Universities (2021BCA02004)

引用格式: 黄沛昱, 宋佳波, 贾洋凡. 基于 FPGA 的高速国密 SM4 光纤通信系统方案[J]. 网络与信息安全学报, 2023, 9(6): 46-55.

Citation Format: HUANG P Y, SONG J B, JIA Y F. High speed national secret SM4 optical fiber communication system scheme based on FPGA[J]. Chinese Journal of Network and Information Security, 2023, 9(6): 46-55.

processes are relatively slow, which hampers their application in scenarios requiring high real-time performance, especially for embedded devices. To address this issue, a high-performance and secure optical fiber communication system was designed based on the FPGA platform and the SM4 algorithm. The FPGA was used to implement the MAC layer interface for SM4 algorithm encryption and decryption, as well as data transmission. Besides, an optimization scheme for the hardware implementation architecture of the SM4 algorithm was proposed. The critical path was shortened by employing a pipeline method, thereby improving the system clock frequency. Additionally, parallel processing of S-box transformation was accelerated to enable efficient data replacement. To reduce data reading delays, a dual-cache processing method was combined to facilitate easier processing of cache data and significantly reduce packet loss rates. This scheme greatly enhanced system data throughput. Experimental results demonstrate that compared to similar designs, the throughput of the SM4 algorithm encryption and decryption module in this scheme reaches up to 25.6 Gbit/s, with minimal differences in resource consumption. Due to limitations imposed by the 10-gigabit SFP+ optical module, the throughput of the entire optical fiber communication system reaches 9.4 Gbit/s. For 128-bit data, the average encryption speed is 0.47 μ s/bit and the average decryption speed is 0.28 μ s/bit, which can be applied to a variety of secure communication scenarios in the internet of things.

Keywords: optical fiber communication, FPGA, data encryption, SM4, pipeline

0 引言

随着现代通信技术和物联网的发展, 工业通信和生活通信需要更高的带宽、更快的速度以及更高的安全性。光纤通信以通信容量大、中继距离长、抗电磁干扰强等特点, 成为现代通信的主要支柱之一, 但光纤通信也存在数据传输的安全性问题。光纤通信主要的窃听方式包括隐蔽式窃听、分离光束、光纤弯曲耦合等^[1], 数据在传输过程中, 一旦被篡改或泄露, 可能造成无法估量的损失。因此, 数据加密在数据传输过程中尤为重要, 特别是物联网的快速发展, 对嵌入式设备的数据安全传输提出了更高的要求。

国际主流的加密算法有高级加密标准 (AES, advanced encryption standard) 算法^[2]、数据加密标准 (DES, data encryption standard) 算法^[3]、RSA (Rivest-Shamir-Adleman) 算法^[4]等。长期依赖国外的加密算法进行国家航天技术研究、国家重大项目数据加解密, 会对我国的数据安全造成严重威胁。为了从根本上摆脱我国对国外密码技术的依赖, 国家密码管理局推出了 SM 系列密码算法, 其中 SM1 集成在芯片中, 没有公开^[5]; SM2 多用于签名验证和加密^[6-7]; SM3 多用于签名验证^[8-10]; SM4 多用于无线局域网和物联网数据加密^[11-13]。将 SM4 算法与现场可编程门阵列 (FPGA, field programmable gate array) 等硬件结合进行光纤通

信数据加解密, 是当下研究热点。

李敏等^[14]提出基于微控制单元 (MCU, microcontroller unit) 将国密 SM4 算法应用在车载设备控制器局域网 (CAN, controller area network) 通信中, 取代 AES 算法实现无钥匙进入及启动 (PEPS, passive entry passive start) 和发动机管理系统 (EMS, engine management system) 安全认证, 该方案加解密时间可达到毫秒级, 有效提高了数据传输效率。Gao 等^[15]提出 SM4 算法硬件实现的循环型和非循环型架构, 循环型架构吞吐量可达 0.54 Gbit/s, 非循环型架构吞吐量可达 20.74 Gbit/s。Zhao 等^[16]采用软硬件结合的方式实现 SM4 算法, 在 Kintex UltraScale 平台上共消耗 1 365 个 LUT (loop up table, 查找表) 和 1 351 个 FIFO 存储器 (first input first output memory), 其吞吐量可达 1.9 Gbit/s。

本文提出 SM4 算法的硬件实现优化架构, 采用流水线、S 盒变换 ROM 并行、双缓存等方式, 设计出基于 FPGA 的高速国密 SM4 光纤通信系统, 使光纤传输具备更快的速度、更高的稳定性和安全性。同时本文针对硬件底层进行开发, 可以通过 UDP/IP 传输数据^[17], 也可以根据实际需求自定义通信协议, 具有通用性, 在实际的产品开发和工程应用中具有较高的价值。

1 系统总体框架设计

开放式系统互联 (OSI, open system inter-

connection) 通信参考模型定义了 7 层网络框架^[18]。本文采用精简的 5 层结构, 将上 3 层(应用层、表示层、会话层) 合并成一个应用层, 保留下 4 层, 内部各功能模块设计遵循该 5 层结构模型约束。

传输层的 UDP 控制模块采用 UDP, 实现数据的 UDP 封装、解封。网络层的 IP 控制模块采用第 4 版互联网协议 (IPv4, internet protocol version 4) 和地址解析协议 (ARP, address resolution protocol) 封装解析, 实现目的 IP 地址的配置以及 MAC 地址的寻址。数据链路层的 MAC IP 核实现 MAC 地址的封装、介质无关接口的连接。物理层的 PCS/PMA IP 核实现 64 bit/66 bit 编码和数据的并/串转换^[19]。

本文设计的光纤通信系统总体框架如图 1 所示。每层的功能模块相对独立, 可各自独立设计, 这种模块化的设计极大地提高了系统的可维护与可拓展性。

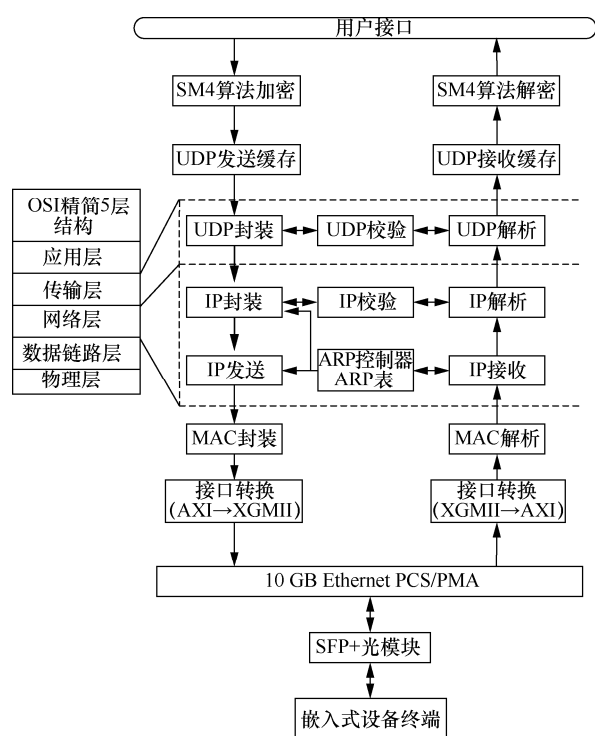


图1 光纤通信系统总体框架

Figure 1 Overall framework of optical fiber communication system

光纤通信加解密可以分成发送和接收两个过程。

发送过程: 应用层数据经过 SM4 加密模块进

行数据加密, 然后通过传输层进行 UDP 包头封装, 再经过网络层进行 IPv4 包头封装以及 MAC 地址的获取, 经过数据链路层进行接口转换, 形成完整的以太网帧之后, 经过物理层的 PCS/PMA 子层实现 64 bit/66 bit 编码和加扰操作, 以及数据的并/串转换, 最后交由发送器通过万兆 SFP+光模块将数据发送给嵌入式设备终端。

接收过程: 嵌入式设备通过 SFP+光模块接收来自主嵌入式设备的数据。数据经过物理层实现并/串转换以及解码, 然后在数据链路层进行接口转换, 随后经过网络层 IPv4 解包和错误检测, 最后通过传输层进行 UDP 解包和 UDP 校验, 在 SM4 加解密模块完成解密, 最终到达指定上层应用。

2 功能模块设计

本文根据 OSI 精简模型进行模块设计。在物理层和数据链路层中使用 10 GB Ethernet MAC IP 核实现 AXIS、XGMII 接口转换; 使用 10 GB Ethernet PCS/PMA IP 核实现 64 bit/66 bit 编码、加扰以及并/串转换; 使用标准的 SFP+光模块实现物理介质关联(PMD, physical media dependent)层接口功能。网络层的 IP_Ctrl 模块实现 IP 帧的封装校验、解析功能; 传输层的 UDP_Ctrl 模块实现 UDP 帧的封装校验、解析功能; SM4 加解密模块实现应用层数据的加解密。FPGA 内部子模块如图 2 所示。

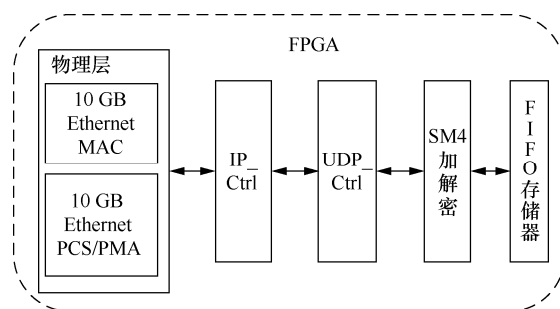


图2 FPGA 内部子模块

Figure 2 FPGA internal submodule

2.1 UDP 封装解析模块

UDP 封装解析模块实现 UDP 封装和 UDP 解析。在封装过程中, 首先从 UDP 发送缓存中读取用户数据, 添加 UDP 包头, 计算校验和, 然后将生成的 UDP 数据包写入 FIFO 存储器, 等待 IP

控制模块读取。UDP 包头由 4 个域组成, 其中每个域各占用 2 byte, 具体包括源端口号、目标端口号、数据包长度、校验值。

UDP 封装过程的状态主要包括 Reset、Idle、Rd_client、Checksum、Write_header 和 Send_data。系统上电进入复位 (Reset) 状态, 然后在 Idle 状态等待命令指示, 当收到读使能信号 Rd_EN, 状态机跳转到 Rd_client 状态读取用户数据, 进入 Checksum 状态计算校验和, Write_header 状态添加 UDP 包头, 最后在 Send_data 状态将 UDP 数据包发送出去, UDP 封装状态转移图如图 3 所示。UDP 解析过程为封装过程的反操作。

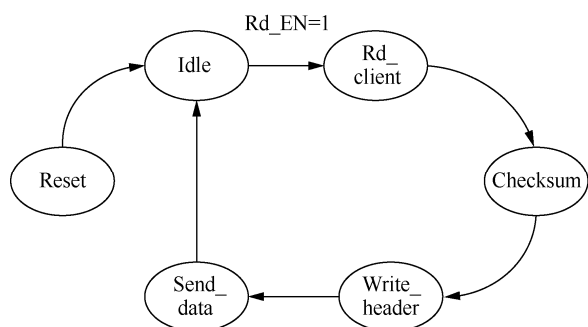


图 3 UDP 封装状态转移图
Figure 3 UDP encapsulation status transition diagram

2.2 IP 封装解析模块

IP 封装解析模块实现 IP 封装和 IP 解析功能。在 IP 封装过程中, 首先从 FIFO 中读取 UDP 数据包, 添加 IP 包头, 计算首部校验和; 然后检测 MAC 变更, 查询 ARP 表, 封装 MAC 首部, 再等待 ARP 控制器确认; 最后将生成的 IP 数据包写入 FIFO 存储器, 等待 MAC 子层读取。IP 包头为固定的 20 byte, 包括版本号、包头长度指示、服务类型、IP 报总长度等。

IP 封装过程的状态主要包括 Reset、Idle、Rd_udpdata、Checksum、ARP_Inquire、ARP_Ask、Write_IPv4、Send_data。系统上电进入 Reset 状态, 然后在 Idle 状态等待命令指示, 当收到读使能信号 Rd_EN, 状态机跳转到 Rd_udpdata 状态读取 UDP 数据包, 进入 Checksum 状态计算校验和, ARP_Inquire 状态通过 ARP 表查询目的 IP 对应的 MAC 地址 (如果 ARP 表中存在该 MAC 地址, 则状态机进入 Write_IPv4, 对数据进行 IPv4 封装; 如果不存在该 MAC 地址, 则通过 ARP_Ask 状态

获取指定 IP 的 MAC 地址), 最后在 Send_data 状态将 IP 数据包发送出去, IP 封装状态转移图如图 4 所示。IP 协议解析过程为封装过程的反操作。

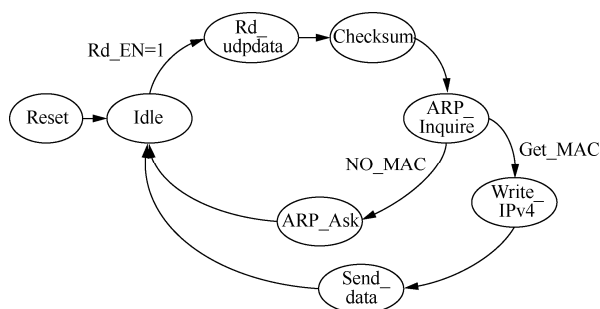


图 4 IP 封装状态转移图
Figure 4 IP encapsulation status transition diagram

2.3 SM4 加解密模块

2.3.1 SM4 原理

SM4 是一种 Feistel 结构的分组密码算法, 其明文长度和密钥长度均为 128 bit。加密算法和密钥扩展算法都为 32 轮非线性迭代。SM4 加解密算法相同, 轮密钥使用顺序相反。SM4 加密过程如图 5 所示, 表 1 为符号说明。

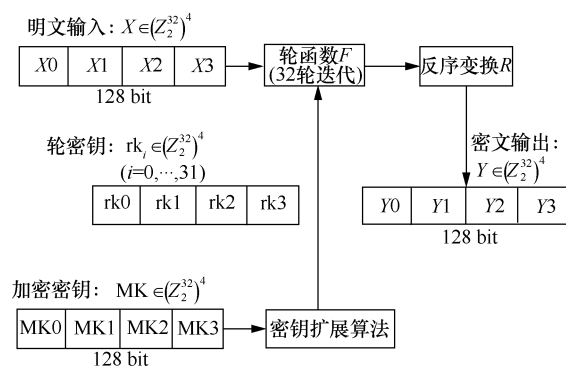


图 5 SM4 加密过程
Figure 5 The encryption process of SM4

轮函数 F : 假设输入为 (X_0, X_1, X_2, X_3) , X_i 为 32 位, 则轮函数 F 为 $F_i = (X_0, X_1, X_2, X_3, rk_i) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk_i)$ 。

合成置换 T : 由一个非线性变换 τ 和线性变换 L 复合而成, 即 $T(A) = L(\tau(A))$ 。

非线性变换 τ : 由 4 个并行的 S 盒构成, 设输入为 $A = (a_0, a_1, a_2, a_3)$, 输出为 $B = (b_0, b_1, b_2, b_3)$, 其中, a_i 和 b_i 为 8 位。 a_i 前 4 位对应的十六进制数作为行编号, 后 4 位对应的十六进制数作为列编号, 然后用相应位置中的字节代替输入

的字节。

线性变换 L : 线形变换的输入就是 S 盒的输出, 即 $C=L(B)=B \oplus (B \ll 2) \oplus (B \ll 10) \oplus (B \ll 18) \oplus (B \ll 24)$, 线性变换的输入和输出都是 32 bit。

反序变换 R : 经过了 32 轮的迭代运算后, 再进行一次反序变换即可得到加密的密文, 即 $C=(Y_0, Y_1, Y_2, Y_3)=R(X_{32}, X_{33}, X_{34}, X_{35})=(X_{35}, X_{34}, X_{33}, X_{32})$ 。

表 1 符号说明
Table 1 Symbol specification

符号	说明
Z_2^e	Z_2^{32} 中, 32 bit 元素称为字, Z_2^8 中, 8 bit 元素称为字节
$Sbox(\cdot)$	S 盒非线性置换函数
$\oplus$	32 bit 异或运算
M_K	加密密钥, 其长度为 128 bit
$\ll i$	32 bit 的循环左移计算
$rk_i(i=0, \dots, 31)$	轮密钥, 其长度为 32 bit
$cki(i=0, \dots, 31)$	固定参数, 其长度为 32 bit

2.3.2 流水线与并行设计

SM4 加密算法的核心是 32 轮非线性迭代, 即轮函数 F , 在硬件上可通过组合逻辑块实现每轮迭代, 轮函数 F 组合逻辑如图 6 所示。

若采用循环迭代结构, 即非流水线方式, 在迭代计算过程中, 第 i 个组合逻辑块 C_i 的输出作为第 $i+1$ 个组合逻辑块 C_{i+1} 的输入。这种非流水线方式只能工作在低速时钟下, 因为其关键路径很长, 提升时钟频率困难。

图 7 为 FPGA 时钟周期的通用计算模型, 时钟周期 $T=T_{co}+T_{logic}+T_{dly}+T_{su}$, 时钟频率 $F_{max}=$

$1/T_{max}$ 。其中, T_{co} 为 D 触发器输出时延, T_{logic} 为组合逻辑计算时延, T_{dly} 为资源布线时延, T_{su} 为 D 触发器建立时间。

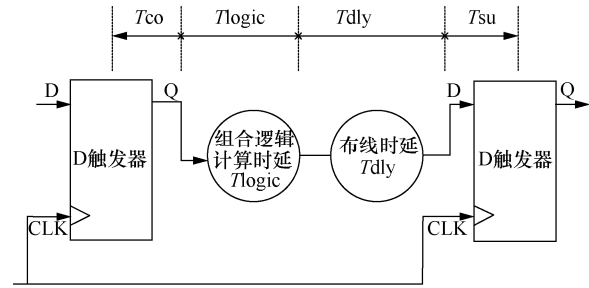


图 7 FPGA 时钟周期的通用计算模型
Figure 7 General calculation model of FPGA clock cycle

对于某一个器件, 其 T_{su} 和 T_{co} 为固定值, 要提高时钟频率, 只需要考虑 T_{logic} 和 T_{dly} 这两个参数。

采用流水线的方式, 在组合逻辑之间插入寄存器可以减小关键路径, 使 T_{logic} 和 T_{dly} 相应减小, 从而提高时钟频率 F_{max} 。所以对 32 轮非线性迭代, 采用 32 级流水线优化设计, 流水线结构如图 8 所示。

SM4 的密钥扩展算法与轮函数迭代结构相似, 也需要进行 32 轮非线性迭代, 主要计算包括异或、合成置换、非线性迭代、循环移位等。在计算第一轮迭代运算的输入时, 需要用系统参数 FK_i 与原始密钥 MK_i 进行异或计算, $MK_i \oplus FK_i = (K_0, K_1, K_2, K_3)$, 然后进行 32 轮迭代。

密钥拓展模块和加密模块可采用并行处理的方式。两模块内部迭代计算均为 32 级流水线, 密钥拓展模块将每轮计算得到的密钥 rk_i 发送给加密模块, 加密模块随即进行一次迭代计算, 经过 32 轮计算后得到 128 bit 密文输出, 并行处理结构如图 9 所示。

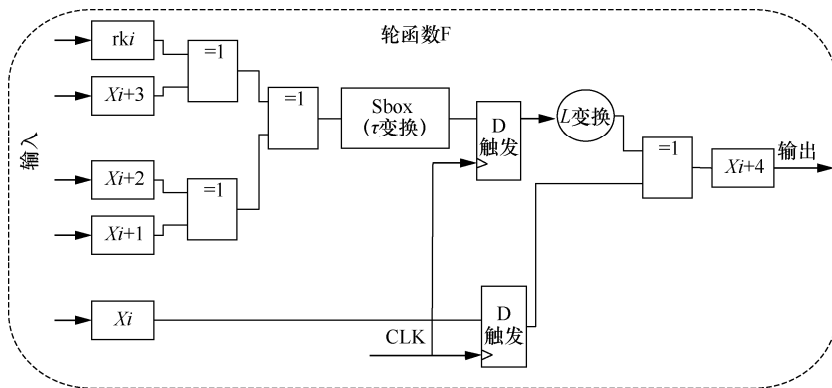


图 6 轮函数 F 组合逻辑
Figure 6 The wheel function F combines the logic

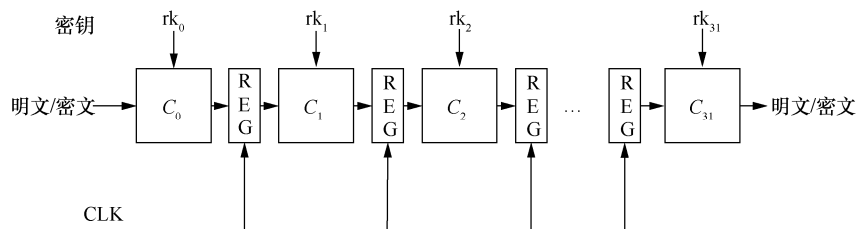


图 8 流水线结构
Figure 8 Pipeline structure

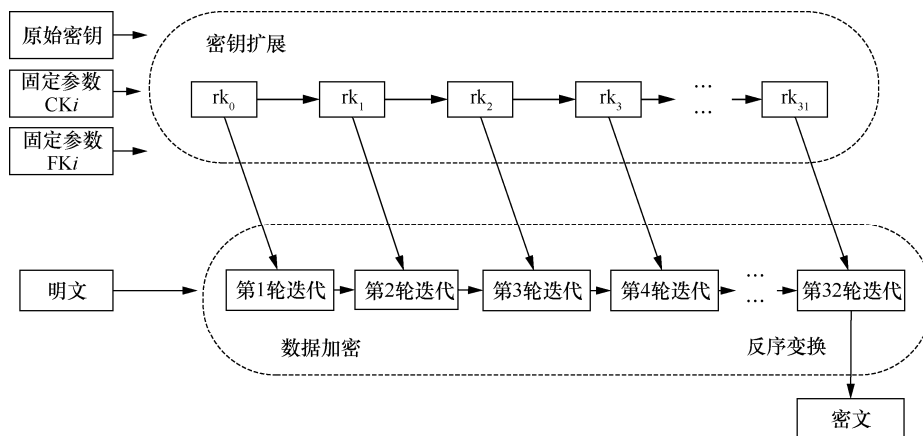


图 9 并行处理结构
Figure 9 Parallel processing structure

2.3.3 S 盒变换 ROM 并行实现

S 盒置换函数是 32 bit 到 32 bit 的映射,按照字节粒度逐字节替换。通过 ROM 查找表的方式实现 S 盒函数,将输入字节 a_0, a_1, a_2, a_3 作为 ROM 的地址,ROM 的数据输出作为 S 盒函数的替换值,ROM 结构如图 10 所示。为了提高加解密处理速度,采用 4 个 ROM 块并行替换输入的 4 个字节,能够在 1 个时钟周期完成 32 bit 数据的替换。

2.3.4 双缓存设计

为了有效地缩短数据加载带来的时延,并且减少外部内存带宽限制带来的影响,采用双缓存设计。双缓存结构如图 11 所示,当缓存区 1 向加解密模块输出数据时,缓存区 2 加载下一次加解

密所需的数据,反之亦然。双缓存结构通过消耗两倍 BRAM 资源的方法,有效缩短了数据传输过程中所带来的时延,从而提高加解密性能。

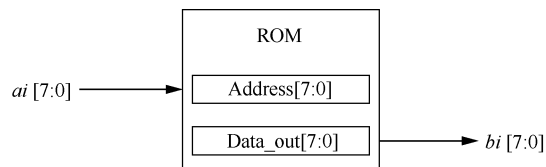


图 10 ROM 结构
Figure 10 ROM structure

与单缓存模式相比,双缓存模式更新缓冲区不会引入中断时延,使用较小的 BRAM 即可满足需求,节约了硬件资源,而且双缓存模式延长了程序处理中断的时间,使缓存区数据的



图 11 双缓存结构
Figure 11 Dual cache structure

处理更加容易,丢包率大大减小。数据的加载和缓冲区数据的处理可以并行执行,系统的实时性得到保证。

3 系统测试分析

本文采用 Xilinx 系列的 XC7Z035-FFG676-2I 器件进行设计实现,使用 vivado 2017.4 工具进行综合、映射和布局布线,使用万兆 SFP+光模块进行数据收发测试。

3.1 资源占用

综合布线后的系统硬件资源总消耗如表 2 所示,主要功能模块硬件资源消耗如表 3 所示。

表 2 系统硬件资源总消耗

Table 2 Total system hardware resource consumption

硬件资源类型	资源总量	实际消耗
DSP	900 个	0 个
BRAM	17.6 Mbit	1.51 Mbit
LUT	171 900 个	9 653 个
FIFO 存储器	343 800 个	10 027 个

表 3 模块硬件资源消耗

Table 3 Module hardware resource consumption

模块名称	BRAM/Mbit	LUT/个	FF/个
UDP 模块	0	202	217
IP 模块	0.11	1 809	2 032
SM4 加解密	1.13	2 017	962

3.2 系统测试方案

本文的系统测试结构如图 12 所示。FPGA A 首先将数据进行 SM4 算法加密、UDP/IP 封装,然后通过 SFP+光模块向 FPGA B 发送 UDP 包。FPGA B 接收到 UDP 包进行 UDP/IP 解析,将解析得到的数据进行 SM4 算法解密,然后经过

FIFO 存储器缓存,通过 ILA 逻辑分析仪抓取解密后的数据。对比 FPGA A 发送的数据和 FPGA B 接收的数据内容是否一致, TX、RX 包数是否一致,由此验证光纤通信加解密系统数据收发的正确性;并通过 SM4 在线加密软件加密,对比本文 FPGA 硬件加密的结果,由此验证 SM4 加解密模块功能的正确性。

3.3 系统性能测试

本文采用米联客开发板进行设计,调用 Xilinx 芯片的 serdes ip 核,对 GTX 链路完整性进行测试,通过 vivado 生成眼图(GTX 信号眼图如图 13 所示),从信号完整性的角度来看,眼图中间的蓝色区域越大, GTX 所对应的 PCB 高速电路的信号完整性越好。因为万兆速率信号的频率相对较高,在传输过程中的损耗较大,上下沿越来越平缓,眼图波形类似于正弦波,该 GTX 链路比较稳定。

对 IPv4 进行测试,通过计算机 ping FPGA, wireshark 软件对 ping 过程的数据进行抓包验证。测试过程中,计算机向 FPGA 发送 ARP 请求, FPGA 能及时响应,返回自身 MAC 地址。IPv4 ARP 连接测试如图 14 所示,能够正常通信。

根据文献[20]中吞吐量的计算公式 $T = \frac{B \cdot f \cdot N}{d}$,其中,吞吐量为 T ,处理数据大小为 B ,系统时钟频率为 f ,流水线的级数为 N ,计算时延为 d 。可以得出本文设计的 SM4 加解密模块吞吐量为

$$T = \frac{B \cdot f \cdot N}{d} = \frac{128 \cdot 200 \cdot 32}{32} = 25.6 \text{ Gbit/s}$$

通过测试方案进行测试,系统吞吐量如表 4 所示。将 UDP 包长分别设置为 16 byte、512 byte、1 000 byte 和 1 472 byte 测试系统吞吐量。受限于

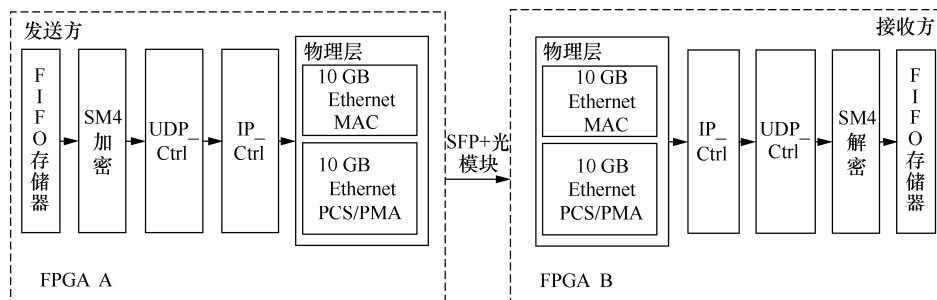


图 12 系统测试结构
Figure 12 System test structure

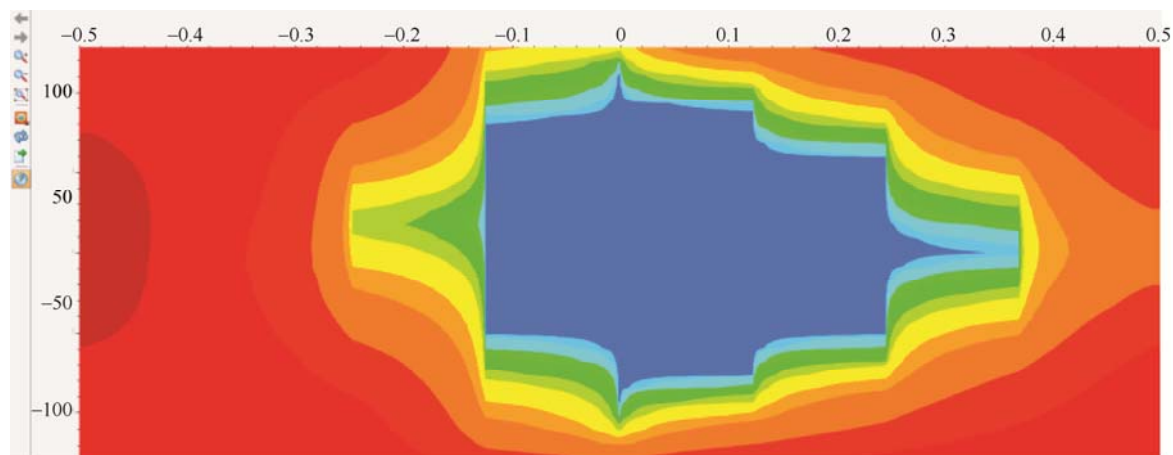


图 13 GTX 信号眼图
Figure 13 GTX signal eye map

Time	Source	Destination	Protocol	Length	Info
1 0.000000	192.168.20.4	192.168.20.3	ICMP	74	Echo (ping) request id=0x0001, seq=8326/34336
2 0.000087	192.168.20.3	192.168.20.4	ICMP	74	Echo (ping) reply id=0x0001, seq=8326/34336
3 1.016055	192.168.20.4	192.168.20.3	ICMP	74	Echo (ping) request id=0x0001, seq=8327/34592
4 1.016187	192.168.20.3	192.168.20.4	ICMP	74	Echo (ping) reply id=0x0001, seq=8327/34592
5 2.040922	192.168.20.4	192.168.20.3	ICMP	74	Echo (ping) request id=0x0001, seq=8328/34848
6 2.041060	192.168.20.3	192.168.20.4	ICMP	74	Echo (ping) reply id=0x0001, seq=8328/34848
7 3.050407	192.168.20.4	192.168.20.3	ICMP	74	Echo (ping) request id=0x0001, seq=8329/35104
8 3.050546	192.168.20.3	192.168.20.4	ICMP	74	Echo (ping) reply id=0x0001, seq=8329/35104
9 4.980813	DhTechno_dc:7a:ea	Xilinx_00:01:02	ARP	42	Who has 192.168.20.3? Tell 192.168.20.4
10 4.980971	Xilinx_00:01:02	DhTechno_dc:7a:ea	ARP	60	192.168.20.3 is at 00:0a:35:00:01:02

图 14 IPv4 ARP 连接测试
Figure 14 IPv4 ARP connection test

万兆 SFP+光模块，当包长达到最大的 1 472 byte 时，整个光纤通信系统吞吐量为 9.4 Gbit/s。

FPGA 发送的 UDP 数据包经过 FPGA B 解包、解密后，数据内容与发送一致，且 TX、RX 包数一致，完成了整个光纤通信加解密系统的链路测试。

表 4 系统吞吐量
Table 4 System throughput

UDP 包长/byte	TX/byte	RX/byte	吞吐量/ (Gbit·s ⁻¹)
16	192 000	192 000	2.0
512	6 144 000	6 144 000	8.4
1 000	12 000 000	12 000 000	9.1
1 472	17 664 000	17 664 000	9.4

通过 ILA 逻辑分析仪抓取 SM4 加密结果，当输入明文为 000102030405060708090a0b0c0d0e0f 时，输出密文为 06989c613da668ad2a8df782e1a8f96a。相同明文使用 SM4 在线加密软件加密，密文一致（不区分大小写，其十六进制值相等），SM4 硬件和软件加密结果分别如图 15 和图 16 所示，说明 SM4 加解密模块功能正确。

本文设计的 SM4 加解密模块，在资源消耗相差不大的情况下，吞吐量比同类型设计更大，SM4 加解密模块性能对比如表 5 所示。对本文方案进行加解密速度测试，将 128 bit 数据加解密 10 000 次取平均值，对比通用 CPU i5-9300 的加解密速度，不同平台加解密平均耗时对比

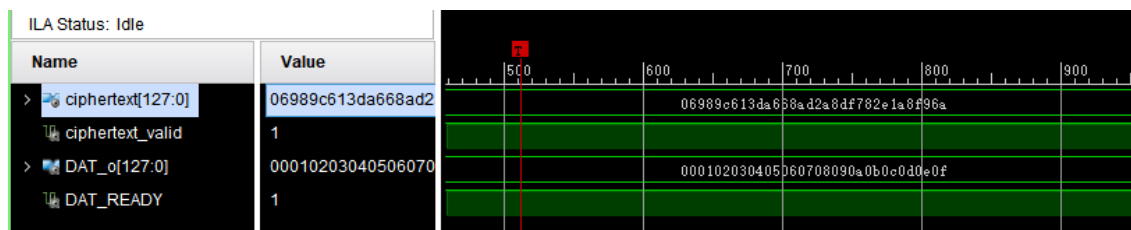


图 15 SM4 硬件加密结果
Figure 15 SM4 hardware encryption result

结果如表 6 所示。

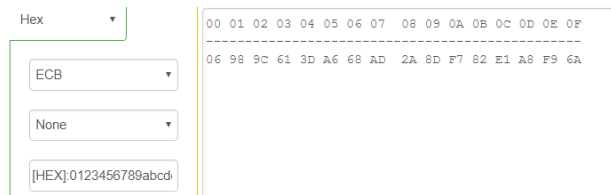


图 16 SM4 软件加密结果

Figure 16 SM4 software encryption result

表 5 SM4 加解密模块性能对比

Table 5 Performance comparison of SM4 encryption and decryption modules

方案	资源消耗	吞吐量/(Gbit·s ⁻¹)	硬件平台
文献[7]	8373 ALM	20.74	Straitx II
文献[8]	1365 LUT 1351 FF	1.9	Kintex UltraScale
本文	2017 LUT 962 FF	25.6	Zynq-7

表 6 不同平台加解密平均耗时对比

Table 6 Comparison of encryption and decryption average time consumed on different platforms

运算类型	测试平台	平均耗时/ μ s
SM4 加密	i5-9300	3.89
	XC7Z035	0.47
SM4 解密	i5-9300	2.51
	XC7Z035	0.28

4 结束语

本文采用国密 SM4 算法, 基于 FPGA 设计了光纤通信系统, 使用硬件实现 SM4 算法加解密以及 MAC 层接口处理。加解密模块采用 32 级流水线、S 盒查找表并行实现和双缓存设计, 有效缩短数据传输过程中所带来的时延, 极大地提高了数据的吞吐量, 从而提升整个通信系统的性能。测试方案结果验证了本文方案功能的正确性和完整性。

实验结果表明, 本文设计的 SM4 算法加解密模块在消耗 2 017 个 LUT 和 962 个 FIFO 存储器的情况下, 吞吐量比同类型设计更大, 能达到 25.6 Gbit/s; 受限于万兆 SFP+光模块, 整个光纤通信系统吞吐量最高为 9.4 Gbit/s; 对 128 bit 数据加密平均耗时为 0.47 μ s, i5-9300 是其耗时的 8.28 倍, 解密平均耗时为 0.28 μ s, i5-9300 是其耗时的 8.96 倍。本文方案针对硬件底层进行开发, 能够根据

不同需求使用不同的传输协议, 可以应用于多种物联网保密通信场景, 尤其是对于加解密实时性要求很高的场景, 在实际的产品开发和工程应用中具有较高的价值。下一步工作考虑在当前方案中添加 SM3 算法, 采用多算法加密提高系统安全性, 同时适用于更多的应用场景。

参考文献:

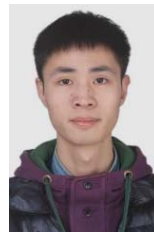
- [1] 连鸿鹏, 程志强, 余丰盈. 光纤通信网络中链路数据篡改攻击与防御方法[J]. 激光杂志, 2022, 43(8): 125-129.
LIAN H P, CHENG Z Q, YU F Y. Link data tampering attack and defense methods in optical fiber communication networks [J]. Laser Journal, 2022, 43(8): 125-129.
- [2] JOSEPH S, SUHAS H S, SUMANTH B K, et al. Implementation of AES algorithm on FPGA and on software[C]//IEEE International Conference for Innovation in Technology (INOCON). 2020: 1-4.
- [3] TIANSHU F, SHUGUO L. A 3DES ASIC implementation with feedback path in the CBC mode[C]//International Conference on Electron Devices and Solid-State Circuits (EDSSC). 2017: 1-2.
- [4] FATEN H M A, HUDA A M, NEVART A M. Speed up image encryption by using RSA algorithm[C]//6th International Conference on Advanced Computing and Communication Systems (IC ACCS). 2020: 1302-1307.
- [5] 刘丁丽, 张大方, 宁佐廷, 等. 基于 SM1 算法的文件安全机制设计与实现[J]. 计算机应用与软件, 2015, 32(12): 316-320.
LIU D L, ZHANG D F, NING Z T, et al. Design and implementation of file security mechanism based on SM1 algorithm [J]. Computer Applications and Software, 2015, 32(12): 316-320.
- [6] 朱辉, 黄煜坤, 王枫为, 等. 一种基于图形处理器的高吞吐量 SM2 数字签名计算方案[J]. 电子与信息学报, 2022, 44(10): 1-10.
ZHU H, HUANG Y K, WANG F W, et al. A high throughput SM2 digital signature computing scheme based on graphics processor[J]. Journal of Electronics and Information Technology, 2022, 44(10): 1-10.
- [7] 刘赣秦, 李晖, 朱辉, 等. 低功耗嵌入式平台的 SM2 国密算法优化实现[J]. 网络与信息安全学报. 2022, 8(6): 29-38.
LIU G Q, LI H, ZHU H, et al. Optimization of SM2 national secret algorithm for low power embedded platform[J]. Chinese Journal of Network and Information Security. 2022, 8(6): 29-38.
- [8] 方轶, 丛林虎, 邓建球, 等. 基于 FPGA 的 SM3 算法快速实现方案[J]. 计算机应用与软件, 2020, 37(6): 259-262.
FANG Y, CONG L H, DENG J Q, et al. Fast implementation of SM3 Algorithm based on FPGA[J]. Computer Applications and Software, 2019, 37(6): 259-262.
- [9] 赵睿斌, 杨绍亮, 王毛路, 等. 基于商密体系的政务链解决数据安全共享交换的研究[J]. 信息安全与通信保密, 2018, (5): 83-88.
ZHAO R B, YANG S L, WANG M L, et al. Research on solving data security sharing exchange by government chain based on business security system[J]. Information Security and Communication Security, 2018, (5): 83-88.
- [10] 周威, 王博, 张卫东. SM3 算法硬件实现研究与应用[J]. 电子测

- 量技术, 2015, 38(12): 67-71.
- ZHOU W, WANG B, ZHANG W D. Research and application of sm3 algorithm[J]. Electronic Measurement Technology, 2015, 38(12): 67-71.
- [11] SA'ED A, REEM J, BASSAM J M, et al. Performance evaluation of the SM4 cipher based on field-programmable gate array implementation[J]. IET Circuits, Devices & Systems, 2021, 15(2): 121-135.
- [12] GUANZY, LLY H, SHANGT et al. Implementation of SM4 on FPGA: trade-off analysis between area and speed[C]//Proceedings of the 2018 IEEE International Conference on Intelligence and Safety for Robotics(ISR). 2018;192-197.
- [13] 王晨光, 乔树山, 黑勇. 分组密码算法 SM4 的低复杂度实现[J]. 计算机工程, 2013, 39(7): 177-180.
- WANG C G, QIAO S S, HEI Y. Low Complexity implementation of Block Cipher Algorithm SM4[J]. Computer Engineering, 2013, 39(7): 177-180.
- [14] 李敏, 陈付龙, 庞辉. 基于国密算法 SM4 的车载 PEPS 和 EMS 安全认证方法研究[J]. 南京信息工程大学学报(自然科学版), 2022, 14(5): 543-550.
- LI M, CHEN F L, PANG H. Research on vehicle PEPS and EMS security authentication method based on SM4[J]. Journal of Nanjing University of Information Science and Technology (Natural Science Edition). 2022, 14(5): 543-550.
- [15] GAO X, LU E, XIAN L, et al. FPGA Implementation of the SMS block cipher in the Chinese WAPI Standard[C]//Proceedings of the 2008 International Conference on Embedded Software and Systems Symposia. 2008: 104-106.
- [16] ZHAO J, GUO Z C, ZENG X W. High throughput implementation of SMS4 on FPGA[J]. IEEE Access, 2019(7): 88836-88844.
- [17] ABHISHEK S, PRAJYANT P. A novel approach for implementing of UDP/IP stack in FPGA[J]. International Journal of Modern Engineering & Management Research. 2017, 5(1): 24-27.
- [18] 郭辉, 罗勇, 郭晓璐. 基于国密算法的车载以太网控制器身份认证方法[J]. 网络与信息安全学报, 2022, 8(6): 20-28
- GUO H, LUO Y, GUO X L. Identity authentication method of vehicle rthernet controller based on national secret algorithm [J]. Journal of Network and Information Security, 2022, 8(6): 20-28.
- [19] 杨钊翔, 孔宪伟, 栾文焕, 等. 基于以太网 10Gbase-R 协议的 PCS 层设计[J]. 微电子学与计算机. 2019, 36(2): 16-20.
- YANG C X, KONG X W, LUAN W H, et al. PCS layer design based on ethernet 10Gbase-R protocol[J]. Microelectronics and Computers, 2019, 36(2): 16-20.
- [20] WANG Y, ZHAO Q, LIEHUI J, et al. Ultra high throughput implementations for MD5 hash algorithm on FPGA[C]//High Performance Computing and Applications. 2010: 433-441.

[作者简介]



黄沛昱(1982-), 女, 四川雅安人, 重庆邮电大学副教授, 主要研究方向为网络通信安全、电子技术应用、FPGA 应用开发。



宋佳波(1996-), 男, 重庆秀山人, 重庆邮电大学硕士生, 主要研究方向为光纤通信安全、密码算法优化实现、FPGA 应用开发。



贾洋凡(2000-), 男, 河北沧州人, 重庆邮电大学硕士生, 主要研究方向为光纤通信安全、密码算法优化实现、FPGA 应用开发。