第 37 卷 第 3 期
2022 年 6 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 37 No. 3
Jun. 2022

DOI:10.13364/j.issn.1672-6510.20210237

基于 SSL/TLS 协议的芯片测试软件平台设计

周卫斌，张达强，毕明帆，胡阳阳，杨永刚
（天津科技大学电子信息与自动化学院，天津 300457）

摘 要：为了保证芯片测试信息在传输过程中的传输安全，基于嵌入式 Linux 技术和 C#编程语言，设计了一种芯片测试软件平台，实现对以海思 Hi3798M V200 高性能芯片为主处理器的封装内系统（SiP）芯片功能测试板卡的测试；通过自主设计使用安全套接字层/传输层安全（SSL/TLS）协议，解决了芯片测试信息在传输过程中容易被伪造和篡改的问题，有效保障测试数据在传输中的安全性；设计了一种线程池方法，进一步提高系统测试效率，节省系统的测试成本. 经分析及验证，该平台实现了芯片测试软件平台的信息安全传输，能够很好地完成对芯片各项功能的测试和验证.

关键词：芯片测试平台；SSL/TLS；OpenSSL；嵌入式 Linux；信息安全；数据加密
中图分类号：TP319 **文献标志码**：A **文章编号**：1672-6510（2022）03-0043-06

Design of Chip Test Software Platform Based on SSL/TLS Protocol

ZHOU Weibin，ZHANG Daqiang，BI Mingfan，HU Yangyang，YANG Yonggang
（College of Electronic Information and Automation，Tianjin University of Science & Technology，
Tianjin 300457，China）

Abstract：To ensure the safe transmission of chip test information during the transmission process, based on embedded Linux technology and C# programming language, we designed a chip test software platform to test the SiP chip function test board with Hi3798M V200 high performance chip as the main processor. In the platform with the use of our independently designed secure socket layer/transport layer security（SSL/TLS） protocol, we resolved the problem that the test information of the chip can be easily forged and tampered with during the transmission process, thus effectively guaranteeing the security of test data during the transmission process; we also designed a thread pool method, which further improved the system testing efficiency, thus saving system testing cost. After analysis and test, the platform achieves the information security transmission of the chip testing software platform, and can well complete the testing and verification of various functions of the chip.

Key words：chip test platform；SSL/TLS；OpenSSL；embedded Linux；information security；data encryption

众所周知，集成电路（integrated circuit，IC）分为设计、制造、封装测试三大环节，封装测试环节是最重要的环节[1]. 集成电路封装测试技术是集成电路发展过程中的三大支撑技术之一；集成电路测试的能力和水平也是集成电路测试产业的重要标志，对半导体行业的发展至关重要[2]. 通过芯片测试可以发现芯片的缺陷，淘汰不合格产品，从而达到规避风险的目的. 目前国内芯片封装测试技术也在飞速发展[3]，但与国外相比还有一定的差距，国际上大型测试公司对其测试设备和测试技术进行封锁，使得国内生产制造的一些高性能芯片也要依靠国外的先进测试技术进行相关测试[4]，这会将我国最新研发的芯片设计制造技术暴露给国外，对我国的国家安全产生很大的威胁. 同时，在目前的芯片测试过程中，通常不对芯片测试的数据进行加密，采用一种明文传输，在通过网络进行芯片测试数据传输的时候，经常会面临很多信息安全问题，如信息欺骗、信息伪造、信息篡改等[5]. 因此，亟须提高国内芯片的测试水平和测试安全性，

收稿日期：2021–11–12；**修回日期**：2022–02–23
基金项目：天津市教委科研计划项目（2018KJ102）
作者简介：周卫斌（1981—），男，湖北孝感人，副教授，zhouweibin@tust.edu.cn

研发高水平的信息安全传输芯片测试系统. 只有这样，才能打破国外垄断，更好地推进芯片行业的安全发展，为我国综合国力的提升注入新的活力[4].

本文设计了一种芯片测试软件平台，实现对以海思 Hi3798M V200 高性能芯片为主处理器的封装内系统(SiP)芯片功能测试板卡的测试，平台采用安全套接字层/传输层安全(SSL/TLS)协议，在网络传输的基础上，使用 OpenSSL 库完成加密[6]；同时设计采用一种线程池方法，可以同时对多块芯片开展测试，能够很好地实现芯片测试系统信息传输的安全性和有效性；整个测试软件平台实行人机互动机制，拥有多种测试模式，系统性能稳定，传输效率较高.

1　芯片测试软件平台总体设计

本文的芯片测试软件平台的测试对象是在以海思 Hi3798M V200 高性能芯片为主处理器的基础上封装完成的自主可控 SiP 芯片功能测试板卡，该板卡以海思 Hi3798M V200 芯片为主体完成硬件设计，主要包括电源模块、时钟模块、存储器模块以及接口模块等. 该芯片测试板卡组成框图如图 1 所示.

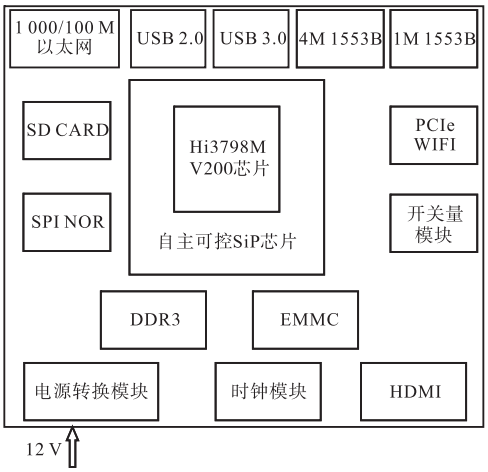

图 1　SiP 芯片功能测试板卡组成示意图

Fig. 1　Composition diagram of SiP chip function test board

1.1　整体框架

芯片测试平台由 3 部分组成：上位机人机交互软件层、信息数据传输加密层以及嵌入式系统测试执行层. 上位机人机交互软件层采用 C#语言编写人机交互界面[7–8]；底层嵌入式系统测试执行层使用 Linux 系统作为操作系统；中间信息数据传输加密层进行芯片测试指令以及芯片数据信息的加密传输，保障芯片测试软件平台能够进行安全有效的测试. 本设计将底层嵌入式系统测试执行层与上位机人机交互软件层分开，实现了远程控制；上位机人机交互软件运行在 Windows 10 Visual Studio 2015 中，底层嵌入式测试系统运行于被测芯片测试功能板卡中；将上位机人机交互软件设置为服务器端，嵌入式测试系统设置为客户端，服务器端下发加密测试指令，客户端执行测试的过程，并将测试完成经过加密的测试数据信息传输到服务器端进行解密和解析，对结果进行显示保存. 整个测试过程可以实时反馈芯片测试的状态信息，完成测试任务，满足测试人员的要求. 芯片测试软件平台的整体通信架构图如图 2 所示.

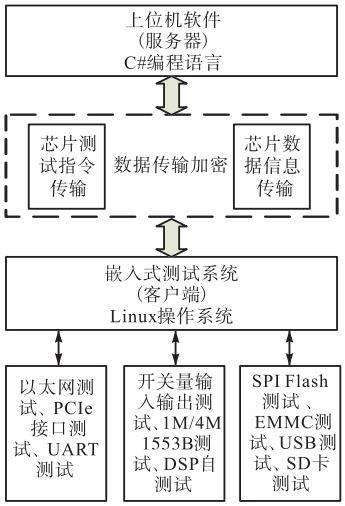

图 2　芯片测试软件平台通信架构

Fig. 2　Communication architecture of chip test software platform

1.2　测试流程

在开展芯片测试时，SSL/TLS 协议负责服务器和客户端的数据传输，在指令数据传输和测试信息数据传输前完成信息加密；然后将信息进行打包，在收到打包信息后进行解密，解析包文件，执行测试和测试信息的反馈. 通过线程池来进行线程的管理，实现一个服务器可以对多个客户端的连接，大大提高了芯片测试平台的效率，芯片测试软件平台工作流程图如图 3 所示.

测试平台的主要测试步骤如下：

(1) 芯片测试人员登录上位机芯片测试平台界面，进行服务器登录，登录成功后进行服务器初始化，等待测试系统客户端的连接. 如果有客户端请求连接，经过验证通过后接受客户端的请求，连接成功.

(2) 选中需要测试的测试项，将指令信息采用 OpenSSL 加密传输至客户端. 客户端进行指令的解

析，执行测试，获取到芯片的测试数据后将测试数据进行加密传输至服务器端；服务器端进行解密操作，执行数据的解析，同时对数据的有效性进行判断，在上位机芯片测试软件界面显示测试的结果信息.

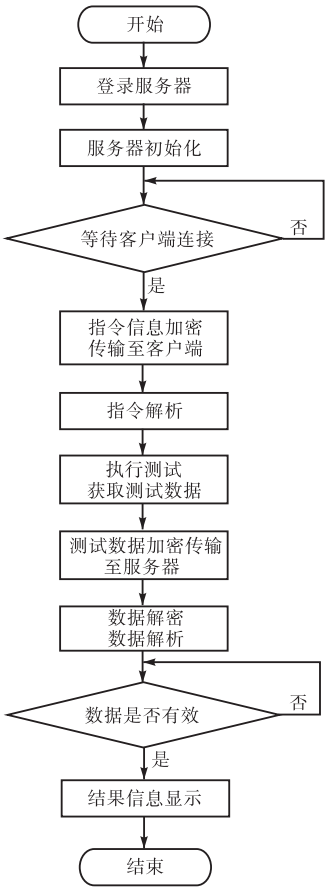

图 3　芯片测试平台工作流程图

Fig. 3　Workflow diagram for chip test platform

2　SSL/TLS 协议

2.1　协议介绍

安全套接字层（SSL）协议[9]最初是网景（Netscape）公司设计的在万维网上获得广泛应用的安全传输协议. 在 1999 年，因特网工程任务组（IETF）设计实现将 SSL 进行标准化（RFC2246）操作，在 SSL 协议的基础上发布了传输层安全（TLS）协议[10]. 目前，SSL/TLS 协议已经成为互联网上被广泛使用的一种安全协议[11].

SSL 协议[12–13]建立在可靠连接（如 TCP 协议）之上，是一个能够防止出现偷听、篡改和消息伪造等安全问题的协议. 它采用一种分层协议，服务器和客户端建立安全的连接，将服务器传输下来的数据进行分片、压缩、计算报文认证码（MAC）、加密，之后将数据发送至客户端；客户端在收到数据后，对信息数据进行解密、验证、解压、重组，完成一次对于信息加密传输的通信过程[12].

在 IOS 七层网络模型中，SSL/TLS 协议处于传输层和会话层之间；在 TCP/IP 网络模型中，SSL/TLS 协议位于传输层和应用层之间[14]. 因此，SSL/TLS 协议将建立一种安全可靠传输的连接，能够防止窃听、篡改和消息伪造，保证信息通信的有效性和可用性.

2.2　SSL/TLS 协议数据加密实现

SSL/TLS 协议为通信的双方建立一条安全的通道，实现数据的机密性传输. SSL/TLS 协议分成记录层和协议高层两部分，记录层指 SSL 记录层协议，协议高层由 4 部分组成，分别是 SSL 握手协议、SSL 密码规范变更协议、SSL 报警协议、SSL 应用数据协议[13]. SSL 记录层协议设计在 TCP 协议之上，可以封装各种高层的应用协议并为高层协议提供一些基本的安全服务，而协议高层则用于实现管理 SSL 的通信.

一个 SSL 记录由两部分构成，包括记录头数据和非零长度数据. 记录头用于指示记录数据的类型和长度，为 3 字节或者 4 字节. 3 字节记录头的最大记录长度为 32 767 字节，4 字节记录头的最大记录长度为 16 383 字节[13]. 握手协议、密钥规范变更协议、报警协议报文需要放在一个 SSL 记录层的记录里，应用数据协议报文可以允许占用多个 SSL 记录层来完成对数据的传送.

SSL 握手协议是 SSL/TLS 协议中最重要的一个协议，该协议用于实现在 SSL/TLS 客户端和 SSL/TLS 服务器端之间鉴别双方的身份，协商加密算法和密钥的参数，建立一条安全的通信通道[15]. SSL 握手协议的类型包括：Client_Hello、Server_Hello、Certification、Server_Key_Exchange、Certification_Request、Server_Hello_Done、Certification_Verity、Client_Key_Exchange、Finished.

整个握手过程分为 4 个阶段：

（1）客户端发起一个请求发送给服务器建立一个安全连接；

（2）服务器进行身份鉴别以及对服务器端的密钥进行交换；

（3）客户端进行身份鉴别以及对客户端的密钥进行交换；

（4）连接完成.

当客户端和服务器端第一次进行通信时，握手协议实现数据在传输过程中的验证，商定服务器端和客

户端使用的加密算法，然后采用加密技术产生共享加密信息或者双方报告错误，将数据进行保护，完成数据传输.

SSL 密码规范变更协议主要包含一条消息，即 Change cipher spec. 当服务器端和客户端协商新的密码规范时，该消息用于通知对方立即开始生效，标志着随后的通信双方交换的是经过加密的密文.

SSL 报警协议为服务器端和客户端通信提供的报警信息有错误、严重、致命 3 种类型；只要有一方发生异常，错误方就会给对方发送一条报警信息.

2.3 OpenSSL

在 SSL 协议中，设计采用了很多手段去保护数据（如对称密码、公钥密码、证书、完成行校验等），从而完成对数据的安全传输. 而 OpenSSL 是一套开源的密码学工具包，很好地实现了 SSL 协议的 SSLv2 和 SSLv3，并且支持 SSL 协议的大部分算法协议[5]，能够提供丰富的应用程序用来进行开发测试，执行数据的加密功能，它能够很好地实现在嵌入式环境下的应用，具有良好的可移植性和可裁剪性. 在本设计中通过使用 OpenSSL 完成对芯片测试平台系统上位机人机交互软件层和嵌入式系统测试执行层之间的信息数据传输加密，以保证数据传输的安全性.

3 测试信息传输设计

3.1 基于 OpenSSL 的传输协议设计

3.1.1 OpenSSL 加密传输模型

传统的芯片测试信息传输系统不能完成信息的加密传输，其在客户端完成对 socket 的创建，利用 connect()进行服务器的连接，recv()/send()接收/发送数据以及 close()关闭连接的功能. 服务器端完成 socket 套接字的创建，IP 地址的绑定，进行端口的监听；然后等待客户端的请求连接，在连接成功后，进行测试数据的接收/发送；最后在数据传输完成后，结束连接.

本设计在传统芯片测试传输系统的基础上，加入 OpenSSL 加密传输协议，使测试数据的传输有了安全保障，在芯片测试数据传输的安全性上有了巨大的改进，能够有效防止数据在传输过程中被窃取和篡改，具有良好的应用性，系统整体框架如图 4 所示.

3.1.2 OpenSSL 客户端加密设计

在 OpenSSL 客户端加密设计时，在原有 TCP 网络通信协议的基础上，增加了 SSL 库的初始化并载入了 SSL 算法以及错误信息. 在 socket 创建完成后，与服务器端进行连接，创建出 SSL 会话环境 SSL_CTX，并将创建好的 socket 加入 SSL 之中，此时便可以建立 SSL 通信，并且利用 SSL 进行芯片测试数据的收发操作；在芯片测试平台测试完成后，进行 SSL 的释放，当测试平台测试完成后系统结束连接，释放 SSL_CTX，客户端的 OpenSSL 加密设计过程如图 5 所示.

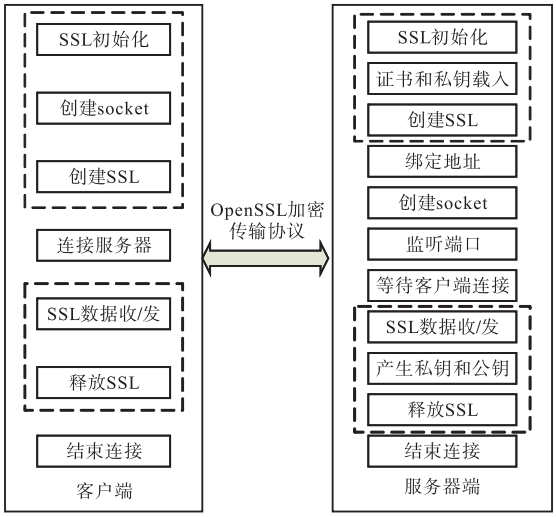

图 4　OpenSSL 加密传输系统整体框架

Fig. 4　Overall block diagram of OpenSSL encrypted transmission system

图 5　OpenSSL 客户端加密设计

Fig. 5　OpenSSL client encryption design

3.1.3 OpenSSL 服务器端加密设计

OpenSSL 服务器端加密设计采用了数字证书和密钥的方法，在芯片测试的过程中能够确保数据传输的安全性. 在通信的过程中，SSL 库进行初始化，载入 SSL 算法和 SSL 错误信息. 建立本次连接所需要使用的协议，申请 SSL 的会话环境 SSL_CTX，载入

用户的数字证书，载入私钥并检查正确性；创建出所需要的 socket 套接字，开启监听，等待客户端发送连接请求. 基于 SSL_CTX 产生新的 SSL，将连接成功的用户加入新的 SSL 中，建立 SSL 连接，完成 SSL 的握手操作；接收芯片的测试数据，进行保存和结果的判断显示. 最后，关闭 SSL 连接，释放 SSL 连接；关闭 socket 套接字，关闭监听 socket，释放 SSL_CTX. 服务器端的 OpenSSL 加密设计的过程如图 6 所示.

图 6　OpenSSL 服务器端加密设计

Fig. 6　OpenSSL server encryption design

3.2　线程池优化设计

3.2.1　工作原理

在操作系统中，进程是操作系统资源分配和调度的最小单位；而线程是 CPU 调度和分配的最小单位，一个优秀的服务器端可以针对多个客户端进行连接操作，进行信息数据的交互，提升系统的工作效率. 因此，本设计中加入了一种线程池优化设计的技术，采用一种多线程任务的开展形式，提前创建好具有一定数目的线程. 当需要新的客户端接入的时候，服务器端可以从提前创建好的线程池中拿出一个当前没有连接任务的线程来处理此任务；当执行测试任务完成后，此线程便放回到线程池中，等待新的客户端连接，这样可以保证多个客户端均可连接服务器端，减少工作的时间.

3.2.2　优点

(1) 节约进程资源. 线程池中所设计的多线程可以实现进程资源的共享，减少了内存以及资源的分配，在创建过程中，进行上下文线程转换的时候可有效节约资源.

(2) 降低成本. 打破传统芯片测试平台一对一测试的瓶颈，采用一对多进行芯片测试，降低了测试的人员成本和硬件成本.

(3) 提高工作效率. 上位机芯片测试软件同时可以针对多块芯片开展测试，能够有效帮助测试人员减少芯片测试工作的时间，大幅度地提高芯片测试平台的自动化控制水平以及人机交互能力，可以直观地发现芯片存在的问题，顺利完成测试任务.

4　平台测试与结果分析

4.1　芯片测试平台结果分析

本设计测试对象是基于海思 Hi3798M V200 高性能芯片为主处理器的 SiP 芯片功能测试板卡，上位机服务器软件登录成功后进入芯片测试平台界面，如图 7 所示. 为此平台设计了 3 种测试模式，分别为单次测试、多次测试、自动测试，可以对芯片的 11 项功能开展测试验证[16]. 单次测试结果如图 8 所示.

图 7　芯片测试平台界面

Fig. 7　Chip test platform interface

图 8　芯片测试平台单次测试结果

Fig. 8　Single test results of chip test platform

在嵌入式 Linux 测试系统中完成交叉编译环境的创建、操作系统和驱动的移植、OpenSSL 的移植，指定 IP 和端口号连接到芯片测试平台开展测试任务[17]. 实验结果表明，该平台能够很好地完成测试数

据信息的加密传输，防止了数据被泄露和被篡改；同时，设计了一种线程池的方法，通过线程池来管理线程，提高了芯片测试的效率.

4.2　安全性分析

SSL/TLS 协议建立在 TCP 传输层之上，在数据传输前已经完成了 SSL 的建立，保证了在数据传输的过程中对数据的加密.

在客户端对服务器端的安全认证过程中，完成对身份的验证，保证是芯片测试人员的操作.

上位机芯片测试软件服务器端对芯片测试结果进行分析认证，在保证安全性的前提下，能够很好地测试验证芯片的各项功能，提高了芯片测试的效率，具有较高的可靠性.

通过测试发现，整个芯片测试软件平台的功能可以正常运行，显示出了良好的测试性能. 同时，通过采用 SSL/TLS 协议对上位机交互界面和底层嵌入式 Linux 测试系统的数据传输进行有效的认证和加密操作，保证了非法用户无法解读或者篡改数据，具有很高的安全性.

5　结　语

本文设计了一种芯片测试软件平台，对以海思 Hi3798M V200 高性能芯片为主处理器的 SiP 芯片功能测试板卡进行测试，对芯片测试过程中数据的安全有效传输进行研究，使用 SSL/TLS 协议设计了数据传输的加密流程，并且移植开源 OpenSSL 实现加密过程，同时设计一种线程池，保证了多个客户端的连接. 该芯片测试软件平台极大地保护了数据安全和信息安全，使测试人员能够准确地把握芯片的状态信息，加速了国内芯片测试平台的良好发展.

参考文献：

[1] 罗和平. 数字 IC 自动测试设备关键技术研究[D]. 成都：电子科技大学，2008.

[2] 俞建峰，陈翔，杨雪瑛. 我国集成电路测试技术现状及发展策略[J]. 中国测试，2009，35(3)：1－5.

[3] 宋武举. 基于 SHC3206 的芯片自动化测试平台设计与实现[D]. 西安：西安电子科技大学，2016.

[4] 杜留根. SPI 接口存储芯片测试系统的设计与实现[D]. 成都：电子科技大学，2021.

[5] 郝克成. 基于嵌入式系统的信息安全传输平台设计[D]. 哈尔滨：哈尔滨工业大学，2006.

[6] 杨柳. 基于 OpenSSL 的文件加密传输系统在 ARM 上的实现[D]. 武汉：武汉科技大学，2016.

[7] 李鸣谦，蓝若明，翟光杰. 基于 C#的超声数据采集系统上位机软件设计[J]. 电子设计工程，2017，25(22)：190－193.

[8] 丁旭. 基于 C#语言与数据库的微波自动测试系统设计[D]. 杭州：浙江大学，2015.

[9] 邓晓军，贺迅宇. SSL/TLS 握手协议的分析与研究[J]. 现代计算机(专业版)，2008(4)：10－12.

[10] ERIC R. SSL 与 TLS：designing and building secure systems[M]. 崔凯，译. 北京：中国电力出版社，2002.

[11] PAUL R，CHAKRABARTI A，GHOSH R. Multi core SSL/TLS security processor architecture and its FPGA prototype design with automated preferential algorithm[J]. Microprocessors and microsystems，2016，40：124－136.

[12] 曾伟. 基于嵌入式 Linux 安全文件传输系统的设计与实现[D]. 武汉：武汉理工大学，2013.

[13] 俸皓. SSL/TLS 在嵌入式系统中的研究与实现[D]. 成都：电子科技大学，2005.

[14] 令晓静. SSL 安全传输协议在网络通信中的应用研究[D]. 西安：西安电子科技大学，2006.

[15] NIKOLOV N，NAKOV O. Research of secure communication of Esp32 IoT embedded system to .NET core cloud structure using MQTTS SSL/TLS[C]//Proceedings of 2019 IEEE XXⅧ International Scientific Conference Electronics(ET). Sozopol：IEEE，2019.

[16] 何友鹏. 基于嵌入式技术的 SIP 专用芯片测试平台研究[D]. 天津：天津科技大学，2017.

[17] 聂和平. 基于 ARM9 的嵌入式 Linux 系统移植与驱动开发[D]. 南京：南京邮电大学，2013.

责任编辑：周建军