基于高性能 FPGA 的超高速 IPSec 安全设备设计与实现

姬胜凯，王　硕，黄毅龙，杨志明，马赋宁，徐　程
（中国电子信息产业集团有限公司第六研究所，北京 100083）

摘　要：基于高性能 FPGA 提出了一种超高速 IPSec 安全设备的设计方案；此方案在以 CPU 作为控制中枢的基础上，利用高性能 FPGA 配合高速接口实现 100G 的 IPSec 安全传输，同时利用高性能 FPGA 和噪声源芯片实现国密算法对高速数据进行加解密。搭建测试环境对样机进行测试，测试结果表明，超高速 IPSec 安全设备可完成高达 82 Gb/s 吞吐率的 IPSec 安全传输，整个系统延时达 90 μs 级。

关键词：超高速；IPSec；FPGA
中图分类号：TN918.4　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097－1788.2024.11.003
引用格式：姬胜凯，王硕，黄毅龙，等. 基于高性能 FPGA 的超高速 IPSec 安全设备设计与实现［J］. 网络安全与数据治理，2024，43(11)：13－18.

Design and implementation of ultra high-speed IPSec security device based on high performance FPGA

Ji Shengkai，Wang Shuo，Huang Yilong，Yang Zhiming，Ma Funing，Xu Cheng
(The 6th Research Institute of China Electronics Corporation，Beijing 100083，China)

Abstract：A design scheme for an ultra high speed IPSec security device based on high-performance FPGA has been proposed. On the basis of using CPU as the control center，this scheme utilizes high-performance FPGA combined with high-speed interface to achieve 100G IPSec secure transmission，while utilizing high-performance FPGA and noise source chip to implement national security algorithm for encryption and decryption of high-speed data. Building a testing environment to test the prototype，the test results indicate that，the ultra high speed IPSec security device can achieve IPSec secure transmission with a throughput of up to 82 Gb/s，and the entire system latency can reach 90 μs level.

Key words：ultra High-speed；IPSec；FPGA

0　引言

近几年来，随着数据中心的建设，用于数据中心间通信的 100G 以太网建设迅速，随之而来的各类网络攻击行为给网络建设带来了挑战，亟需部署网络安全设备进行网络安全防护，目前主要部署网络密码机进行数据安全防护，对传输数据提供机密性、完整性和不可否认性保护。目前超高速 IPSec 密码机协议栈多基于大型 CPU 使用 DPDK 技术实现，软件方式实现的 IPSec 协议大大增加网关的负载，成为网络的瓶颈[1]，而 FPGA 具有高速并行的特点，可实现超高速的 IPSec 处理。基于高性能 FPGA 的 IPSec 安全设备的实现，可以满足 100G-IPSec 协议栈超高速、超高吞吐量、极低时延和较多隧道数的特性。

1　IPSec 协议

IPSec 是为 IP 网络提供完整安全性解决方案的一系列服务和协议的集合[2]。IPSec 协议的结构文档 RFC2401，定义了 IPSec 的基本结构，定义了 IPSec 提供的安全服务等。IPSec 协议是一组用于 IP 层上提供身份认证、数据完整性、重放保护和加密的协议扩展，包括 AH 和 ESP 两个安全协议，以及为安全协议协商参数的密钥管理协议[3]。IPSec 协议提供两种不同的封装模式，传输模式用于保护上层 IP 数据包的有效载荷，隧道模式用于保护整个 IP 数据包，包括其头部信息。

（1）安全联盟。安全联盟（Security Association，SA）是通信实体之间经过协商建立起来的单向的逻辑连接，包含用于确定使用何种协议来保护数据，使用何种算法，加密和认证方式，加密认证密钥，是否启用抗重放服务以及抗重放服务序列号，安全联盟生存期等信息[4]。SA 是 IPSec 协议保护的基础，AH 协议和 ESP 协议基于 SA

实现保护，IKE 协议主要是为了建立和维护 SA[5]。

（2）IKE 协议。设备使用 AH/ESP 协议保护数据包时，需要通过共享信息实现互相通信互相识别。IKE 协议为实现 IPSec 通信的端口之间提供共享状态信息协商，为两个参与方提供相互认证，建立 IKE SA，共享秘密信息以建立 ESP/AH SA，协商 SA 使用的加密算法以保护承载的流量[6]。

（3）AH 协议。AH 协议提供无连接的数据完整性校验、数据来源认证和可选的抗重放保护。AH 的保护范围从 IP 头开始，到上层协议载荷结束；IP 包在传输过程中，有些字段可能会变化，且接收方不可预测，这些字段不被 AH 协议保护。

（4）ESP 协议。ESP 协议除提供 AH 协议所包含的保护外，还提供数据机密性保护。在数据机密性保护方面，ESP 协议为上层载荷提供保护；在数据完整性和数据源认证保护方面，ESP 协议提供从 ESP 头开始，包含上层协议头、上层协议载荷，到 ESP 尾结束的保护范围[7]。

2　设计与实现

2.1　架构设计

现阶段针对传统 IPSec 安全设备的研究中，常采用并行化技术来提升性能，主要包括加密技术的并行化和高速报文传输并行化。加密过程常采用两种并行方式对其性能进行优化，一是加密认证算法本身处理流程并行化；二是借助于多处理器或 FPGA 等其他加速硬件使实现密算法和协议处理并行化。近些年来，针对内核处理低效问题，研究人员设计了很多框架来加速报文处理。这些框架分为两类，一类偏向使用硬件例如 GPU 或 FPGA 等辅助 CPU 进行处理；一类偏向使用软件，绕开内核报文收发和内核协议栈，使用高性能报文收发平台和用户态协议栈加速报文处理[8]。本文方案选择高性能 FPGA 实现 100G 速率的 IPSec 数据接入、协议处理及加解密算法，并且可支持 100G 以太网高速接口。

数据处理逻辑架构如图 1 所示，以高性能 FPGA 为基础，接口单元通过 FPGA 完成 100G 数据的接入、数据的收发、IPSec 解析与封装，算法处理单元通过算法 FPGA 实现数据的加密解密处理，管理单元完成设备管理、密钥协商等功能。

超高速 IPSec 安全设备实现网络数据的高速处理，解决高速数据接入、超高速网络协议处理及超高速密码算法实现的性能瓶颈。当内网接口内 FPGA 接收到 100G 数据流量后，由硬件逻辑实现 IPSEC 解析与封装，将数据流量发至算法 FPGA 进行加密处理，处理结束后发至外网接口，进行数据封装和转发。数据在加密方向上经过了内网接口 FPGA→加密算法 FPGA→外网接口 FPGA；在解密方向上经过了外网接口 FPGA→解密算法 FPGA→内网接口 FPGA。

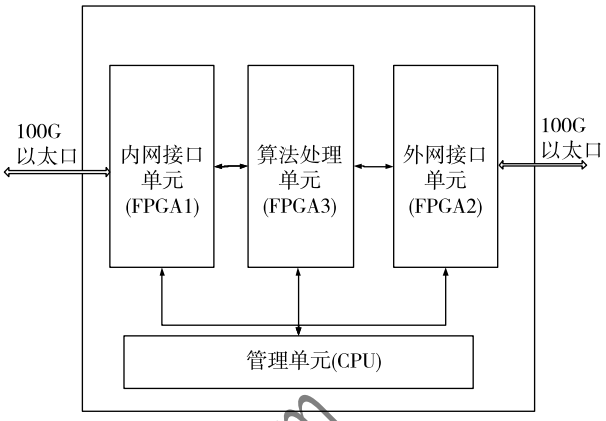


图 1　系统架构框图

超高速 IPSec 安全设备使用安全隔离设计关键技术提高设备的安全性，为提高超高速 IPSec 安全设备的抗网络攻击和安全隔离的能力，架构上内网接口单元和外网接口单元选用不同元器件，内外网接口相互独立的设计有效地把外网数据和内网数据隔离开，提高抗网络攻击的能力。

2.2　内外网接口单元设计

IPSec 设备在接口单元上，最核心的器件就是实现 100G 接入及处理功能的芯片和 CPU。目前常用的实现 100G 数据接入功能的方案有三种：通过 CPU 接入、专用 ASIC 的专用 100G 接口接入、使用 FPGA 提供 100G 接口接入。三种接口芯片选择特点如下。

（1）基于 CPU 通过软件 100G 接入

高性能 CPU 可提供 100G 接口，通过 DPDK 协议软件实现 100G 接入，这种接入方式需要依赖软件实现，性能很难达到要求。根据公开的测试报告，基于以下配置：Intel 16 核 Xeon D-1571，64 GB DDR4-2133，主板 supermicro X10SDV-7TP8F，接入 100G 以太网时，通过 DPDK 实现 VPN 处理，吞吐率在 1 400 字节包长时，吞吐率≤80 Gb/s，64 字节长时，吞吐率≤20 Gb/s，性能相对不高。由于 IPSec 工作在网络层，需与协议栈高度耦合，基于高性能 CPU 通过软件方式实现的 IPSec 协议大大增加了安全设备的负载，成为网络的瓶颈，且 CPU 安装有操作系统，很难做到网络安全隔离，存在有网络攻击风险。

（2）通过专用 ASIC 实现 100G 接入

常用网络接入 ASIC 芯片是交换芯片，网络交换设备多使用博通公司的 BCM82332 交换芯片，可实现 100G 数据的接入，但还需选取相应的数据处理处理单元，并使用该交换芯片实现 IP 数据接入，存在报文乱序、数据

流向不可控的风险，且通用网络交换芯片有被攻击的风险。

（3）FPGA 逻辑实现

应用高性能 FPGA 实现 100G 接口，通常使用 Xilinx 公司的 XCVU9P FPGA，利用芯片自带的 100G MAC 提供 100G 接口（QSFP28），可完成 100G 数据接入，并且报文顺序和数据流向可控，且使用 FPGA 实现数据接入，该芯片不带操作系统，可有效进行网络攻击的报文的隔离和过滤。

通过比较分析，超高速 IPSec 安全设备的内外网接口芯片选择高性能 FPGA，能够在保证数据有效接入的情况下，提供较高的安全隔离能力。

2.3 硬件设计

100G 超高速 IPSec 安全设备硬件设计如图 2 所示。

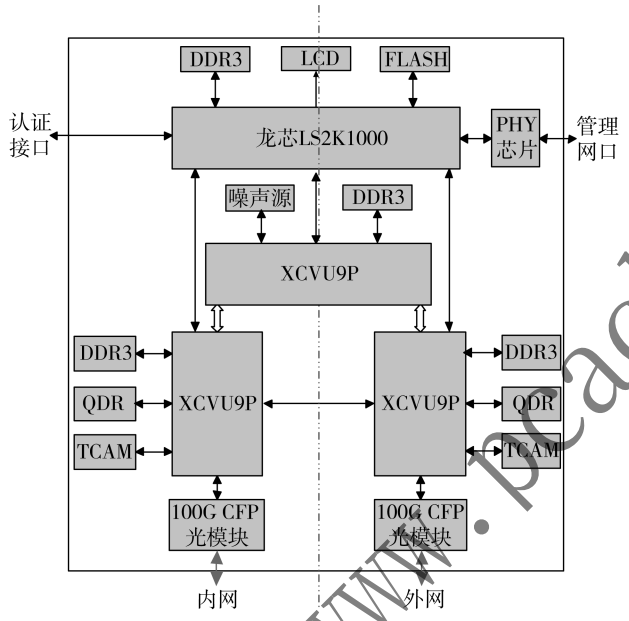


图 2　超高速 IPSec 安全设备硬件设计图

100G 超高速 IPSec 安全设备接口单元通过 FPGA 完成 100G 数据的接入、数据收发、IPSec 解析与封装，以 Xilinx 公司的 XCVU9P FPGA 为基础，该型号 FPGA 为 Xilinx 的高端 FPGA，使用 16 nm Fin FET 工艺，拥有丰富的可编程逻辑、DSP 资源以及存储资源，带有 9 个 100G 的接口。表 1 列出了 VU9P FPGA 的各项片内资源。

100G 超高速 IPSec 安全设备的管理单元主要实现密钥协商、设备管理等功能，由于该处理器需要完成建立链路的链接和密钥协商，对性能有一定要求，因此选用龙芯 LS2K1000。龙芯 LS2K1000 基本性能如下：内核，GS264 双核；主频，1 GHz；内存，DDR3 位宽 64 位；接口，PCIE、USB、以太网口、UART、IIC 等。综合评估，LS2K1000 能够满足应用需求。

表 1　XCVU9P FPGA 内部资源

名称	XCVU9P
System Logic CELLS	2 586 150
CLB Flip-Flops	2 364 480
CLB LUTs	1 182 240
Max. Distributed RAM/Mb	36.1
Block RAM Blocks	2 160
Block RAM/Mb	75.9
UltraRAM Blocks	960
UltraRAM/Mb	270.0
CMTs（1 MMCM and 2PLLs）	30
MAX. HP I/O	832
DSP Slices	6 840
System Monitor	3
GTY Transceivers 32.75 Gb/s	120
Transceiver Fractional PLLs	60
PCIe Gen3 ×16 and Gen4 ×8	6
150G Interlaken	9
100G Ethernet w/RS-FEC	9

噪声源芯片选用 WNG-8，是一种数字物理噪声源，主要用于产生真随机序列，是算法处理单元不可缺少的基础部件。

2.4 系统软件设计

100G 超高速 IPSec 安全设备软件上主要包括 IKE 模块、IPSec 通信模块和 IPSec 加解密模块。为了保证数据流在经过设备的加密处理后仍能保持较高的收发速率，本文基于高性能 FPGA 多核架构实现用户态 IPSec。从功能实现上分为以下几个部分。

（1）IKE 模块：IKE 协商模块负责 IPSec VPN 隧道的工作密钥和会话密钥的协商、更新、销毁及隧道状态监控。提供基于五元组（源 IP 地址、目的 IP 地址、源端口号、目的端口号、协议号）分配不同的会话密钥的功能。

（2）IPSec 通信模块：IPSec 通信模块负责维护 IPSec 安全通信策略、会话密钥；对加密报文进行 IPSec 隧道封装，对解密报文进行解封装处理。同时将待加解密数据发送到 IPSec 加解密模块。

（3）IPSec 加解密模块：IPSec 加解密处理，负责对报文进行加密运算和解密运算，IPSec 加解密功能中，公钥算法采用国密 SM2，杂凑算法采用国密 SM3，分组密码算法采用国密 SM4。

超高速 IPSec 安全设备的数据传输加密功能由 FPGA 逻辑实现，包括接口 FPGA、算法 FPGA，逻辑设计总体架构如图 3 所示。

加密方向的处理流程依次包括：报文解析（内网接收）、二层分类、分片重组、五元组查找、策略提取、IPSec 协议封装、加密算法、IP 包重构、以太帧重构以及网

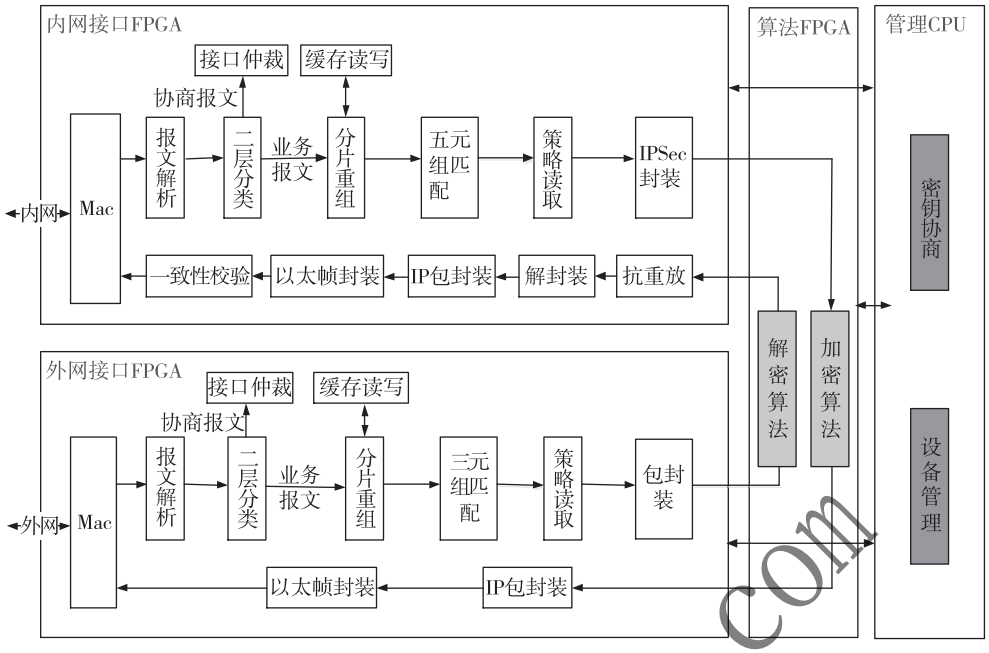


图 3　超高速 IPSec 数据流程图

络发送接口（外网发送）等功能模块。

解密方向的处理流程依次包括：报文解析（外网接收）、二层过滤、分片重组、三元组查找、策略提取、包封装（参数携带）、解密算法、抗重放、IP 包重构、以太帧重构、一致性检查、网络发送接口（内网发送）等功能模块。

超高速 IPSec 安全设备算法 FPGA 进行密码算法运算时，数据传输单元与算法核单元属于串行结构，算法核需等待数据输入完成后启动加解密，数据输出单元需等待数据加解密完成后启动数据输出，单一的算法核能够提供的加解密算法运算速率有限，其数学模型符合木桶原理，数据传输、数据加解密等每一个阶段的效率都是限制整体加解密速率的瓶颈。为提高超高速 IPSec 安全设备数据加解密的处理性能，设计采用多个对等算法核同时进行运算，即“并发工作”，有效提高加解密模块处理性能，提高业务数据加解密吞吐率；为解决多算法核对数据传输单元的争用问题，设计多级流水线工作模式，在实现的过程中加强时钟约束，实现算法核的并行处理，数据传输单元的高位宽高工作主频处理，提高加解密模块各功能单元的利用效率。

3　实验验证

根据硬件设计完成超高速 IPSec 安全设备样机研制，为了验证样机设计的可行性并测试加解密功能，搭建了如图 4 所示的功能测试网络环境。测试终端：CPU，Intel 2. 0GHz 以上；内存，32 GB；配备 100G 网卡。

功能测试步骤：

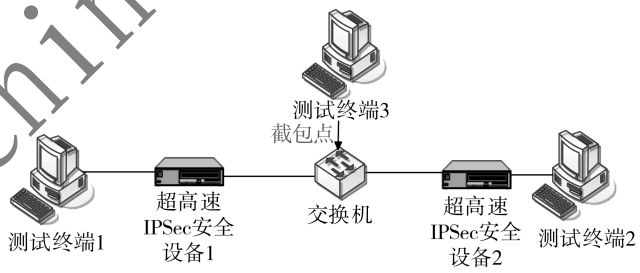


图 4　功能测试环境

（1）配置安全设备 1 和安全设备 2 的 IPv4 传输模式。

（2）使用测试终端 1 和 2 进行互 ping，同时在截包点抓取报文，核对抓到报文包封装格式为 ESP。

（3）在终端 1 和 2 上运行 FileZilla 软件使用 FTP，进行 4 GB 文件传输，查看文件传输情况。

（4）配置安全设备 1 和安全设备 2 的 IPv4 隧道模式。

（5）使用测试终端 1 和 2 进行互 ping，同时在截包点抓取报文，核对抓到报文包封装格式为 ESP。

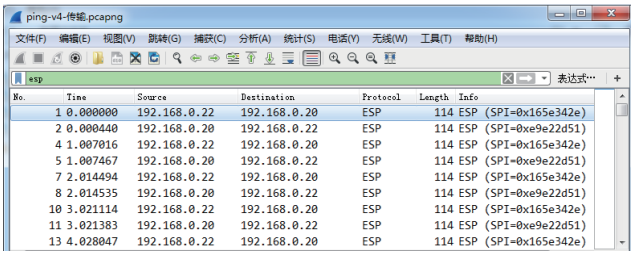
（6）在终端 1 和 2 上使用 FTP 运行 FileZilla 软件，进行 4 GB 文件传输，查看文件传输情况。

（7）配置安全设备 1 和安全设备 2 的 IPv6 业务，重复步骤（1）~步骤（6）的测试。

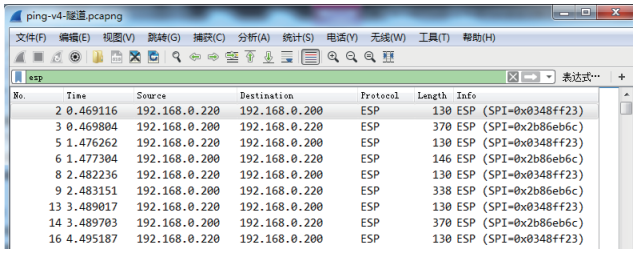
功能测试情况如图 5、图 6 所示，经测试，超高速 IPSec 密码机在 IPv4/IPv6 下均能够正确进行 IPSec 加解密处理。

为了验证样机设计的可行性并测试相关的性能参数，搭建了如图 7 所示的性能测试网络环境，使用思博伦 C50 网络测试仪进行性能测试，该型思博伦网络测试仪带 2

(a) IPv4 ping通信正常

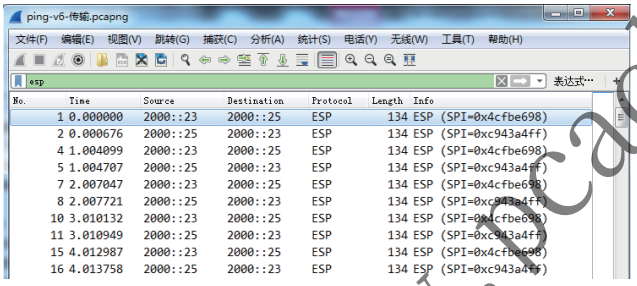


(b) IPv4 ping包传输模式密文

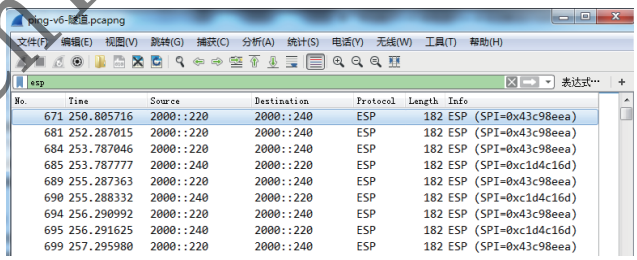


(c) IPv4 ping包隧道模式密文

(d) IPv6 ping通信正常



(e) IPv6 ping包传输模式密文



(f) IPv6 ping包隧道模式密文

图 5　ping 通信测试结果

个 100G-QSFP28 光口，提供网络第 2 至 3 层流量产生和分析能力。

性能测试步骤：

（1）为安全设备 1 和安全设备 2 配置 IPv4 隧道模式。

（2）运行网络测试仪软件，按照 RFC2544 标准对两台设备之间的加解密吞吐率进行双向连续 1 分钟、包长 1 400 字节数据包测试。

（3）记录加解密吞吐率和加解密时延。

（4）为安全设备 1 和安全设备 2 配置 IPv6 隧道模式。

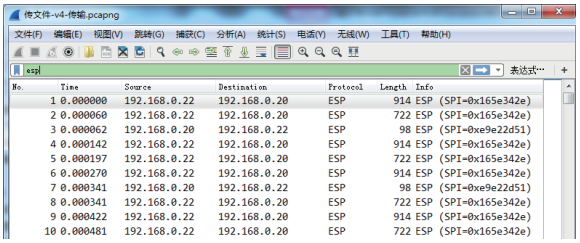
（5）运行网络测试仪控制软件，按照 RFC2544 标准对两台设备之间的加解密吞吐率进行双向连续 1 分钟、包长 1 400 字节数据包测试。

（6）记录加解密吞吐率和加解密时延。

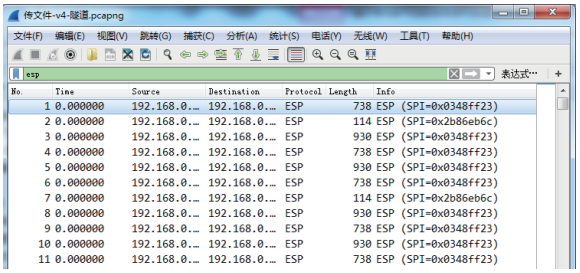
按照测试步骤分别在 IPv4 和 IPv6 网络下测试隧道模式下的加解密吞吐率性能，性能测试结果如图 8、图 9 所示，经测试，超高速 IPSec 安全设备在隧道模式下，IPv4 加解密吞吐率可达 85.938 Gb/s，整个系统延时为 89.079 μs，IPv6 加解密吞吐率可达 82.422 Gb/s，整个系统延时为 90.825 μs。

4　结论

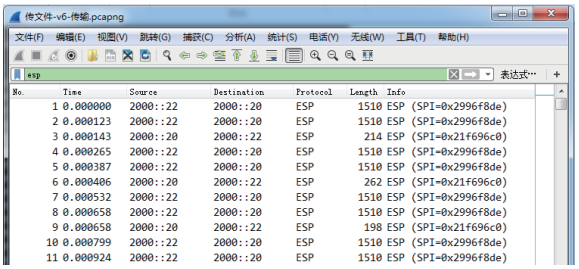
本文通过对超高速 IPSec 安全设备的研究与设计，利用高性能 FPGA 完成了 100G 高速网络接口模块的设计和实现，同时利用高性能 FPGA 和噪声源芯片实现国密算法对高速数据进行加解密，保证了高速网络传输过程中数据的安全。通过搭建的测试环境对超高速 IPSec 安全设备进行测试，测试结果表明，该设备支持 IPv4 密通和 IPv6 密通，并可完成高达 82 Gb/s 有效数据的安全传输，整个系统延时达 90 μs 级，能够满足 100G-IP 网络的安全防护需求。综上所述，该方法对解决超高速网络数据传输中存在的超高速 IPSec 密码机的实现问题具有较高的参考价值。



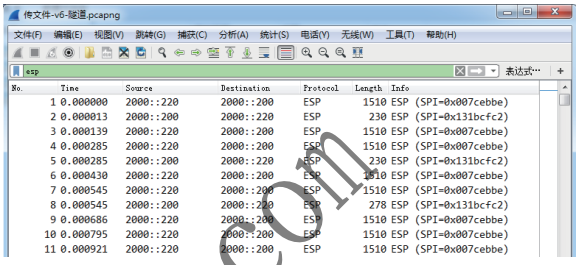
(a) IPv4传文件传输模式密文



(b) IPv4传文件隧道模式密文



(c) IPv6传文件传输模式密文



(d) IPv6传文件隧道模式密文

图 6　FileZilla 传输文件测试结果

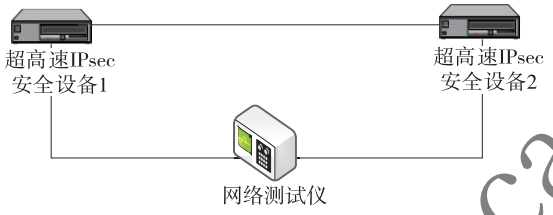


图 7　性能测试网络环境

Id	Configured Frame Size	Intended Load (%)	Result	Throughput (%)	Minimum Latency (us)	Maximum Latency (us)	Average Latency (us)
0	1.400	10	Passed	10	82.83	88.01	83.294
1	1.400	55	Passed	55	83.54	96.74	85.33
2	1.400	77.5	Passed	77.5	83.65	95.92	86.593
3	1.400	88.75	Failed	0	84.36	300.71	251.373
4	1.400	83.125	Passed	83.125	84.37	97.98	87.472
5	1.400	85.938	Passed	85.938	84.48	97.79	89.079
6	1.400	87.344	Failed	0	83.29	300.28	248.013
7	1.400	86.641	Failed	0	84.6	300.5	247.26

图 8　IPv4 隧道模式性能测试结果

Id	Configured Frame Size	Intended Load (%)	Result	Throughput (%)	Minimum Latency (us)	Maximum Latency (us)	Average Latency (us)
0	1.400	10	Passed	10	85.87	89.15	86.388
1	1.400	55	Passed	55	86.45	101.06	89.465
2	1.400	77.5	Passed	77.5	87.94	101.51	89.925
3	1.400	88.75	Failed	0	88.4	332.73	276.942
4	1.400	83.125	Failed	0	88.02	101.37	90.649
5	1.400	80.313	Passed	80.313	86.76	101.71	90.374
6	1.400	81.719	Passed	81.719	87.91	101.19	90.426
7	1.400	82.422	Passed	82.422	88.01	101.78	90.825

图 9　IPv6 隧道模式性能测试结果

参考文献

[1] 李曦. 基于高性能 FPGA 芯片的千兆网 IPSec 协议模块 [J]. 计算机工程与应用，2005（19）：162－165.

[2] 刘振钧，李治辉，林山. 基于 FPGA 的万兆网的 IPSec ESP 协议设计与实现 [J]. 通信技术，2015，48（2）：242－246.

[3] 邹新一. 面向云服务的高性能安全接入网关的研究与实现 [D]. 哈尔滨：哈尔滨工业大学，2018.

[4] 朱永升. IPSec 技术研究及其在路由器上的实现 [D]. 西安：西安电子科技大学，2007.

[5] PARK J，JUN A. A lightweight IPSec adaptation for small devices in IP-based mobile networks [C]//2006 8th International Conference Advanced Communication TechnologyPhoenix Park. IEEE，2006.

[6] 谢建豪. IPSec 下 IKEv2 协议的研究与实现 [D]. 西安：西安电子科技大学，2015.

[7] OGUDO K A. Analyzing Generic Routing Encapsulation（GRE）and IP Security（IPSec）tunneling protocols for secured communication over public networks [C]//2019 International Conference on Advances in Big Data，Computing and Data Communication Systems（ic ABCD）. IEEE，2019.

[8] 穆瑞超. 基于 DPDK 的高性能 VPN 网关的研究与实现 [D]. 哈尔滨：哈尔滨工业大学，2017.

（收稿日期：2024－08－27）

作者简介：

姬胜凯（1990－），男，硕士，工程师，主要研究方向：信息安全、安全系统设计。

王硕（1988－），男，硕士，工程师，主要研究方向：信息安全、FPGA 软件设计。

黄毅龙（1988－），男，硕士，高级工程师，主要研究方向：信息安全、电子信息。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部