Some issues about upgrading and developing high-speed local IP network encryption devices

Tran Van Khanh, Nguyen Van Tu

***Abstract*—In this article on the basis of researching technological solutions to design and manufacture IP network encryption devices in the world, the authors synthesized and introduced the trend of developing technologies for IP network encryption devices, simultaneously explained the challenges posed in the design and manufacture of local IP network encryption devices, proposed design and manufacturing models to ensure optimization based on PowerPC and FPGA solution . The proposed model has been applied in designing and manufacturing IP network encryption devices.**

***Tóm tắt*—Trong bài báo này, trên cơ sở nghiên cứu về các giải pháp công nghệ trong việc thiết kế chế tạo các hệ thống bảo mật luồng IP trên thế giới, nhóm tác giả đã tổng hợp và đưa ra xu hướng phát triển các hệ thống bảo mật mạng IP đồng thời luận giải về các thách thức đặt ra đối với các hệ thống bảo mật mạng IP nội địa, đề xuất giải pháp nâng cấp,thiết kế chế tạo đảm bảo tính tối ưu dựa trên nền tảng công nghệ PowerPC kết hợp với FPGA. Giải pháp đề xuất đã được ứng dụng trong việc thiết kế, chế tạo một số dạng hệ thống bảo mật mạng IP trong thực tế.**

***Keywords*—IP network encryption device; PowerPC; FPGA .**

***Từ khóa*—Hệ thống bảo mật luồng IP; Power PC; FPGA.**

I. INTRODUCTION

The development of telecommunications technology in the country and in the world is generally developing along the path towards IP convergence. In addition to IP transmission (over the Internet / not over), we can clearly see the evolution from ATM asynchronous networks (Asynchronous Transport Mode) to synchronous optical network SONET (Synchronous Optical Network), a hierarchical data system. Synchronous Digital Hierarchy (SDH) and, most recently, Ethernet and optical innovations.

Along with the strong and widespread development of the Internet is the emergence of more and more needs for information security and safety. In the market, IP network encryption products are increasingly rich in quantity and increasing in quality, such as ANIS, Premium of CE-Infosys, Cipher X 7211, Cipher X 7220 of TCCsecure, DATACRYPTO 5000 Series of Thales, R&S®SITLine ETH by Rohded&Schwarz...

However, the strong development of the IoT technology development trend of the 4.0 technology revolution, especially the increase in the number of user applications and data traffic, has been posing development needs. new in the field of network technology development in general and security in particular. This not only promotes the networking industry to continuously innovate to increase communication speed and reduce energy consumption, but also promotes the development of security, safety and security services for high-speed IP network encryption devices.

Old generation domestic IP network encryption products, in many cases, no longer meet the needs of processing speed, connectivity, safety and security of the execution algorithms as well as requirements for configuration, management, monitoring. Upgrading performance, safety, security or additional features on configuration, monitoring management requires thorough research and comprehensive system not only in terms of choosing the right technology. solution technology to achieve the desired performance and features, taking into account factors of system compatibility for the systems being deployed.

II. DEVELOPMENT TREND OF IP NETWORK SECURITY TECHNOLOGY AND PROBLEMS FOR LOCAL IP SECURITY TECHNOLOGY

There are many IP network security products on the world market. However, in terms of solutions, they can be divided into three groups::

Group 1: Completely secure by hardware engineering.

Group 2: Combining the use of hardware and software in security solutions.

Group 3: Completely using software security solutions.

A software-based security product, usually installed in operating systems using CPU-centric processing chips, and has the advantage of being flexible, easy to install, easy to upgrade, easy to customize, however, speed low handling.

The product group that combines hardware and software takes advantage of both advantages of technology, being both highly customizable, and has good speed and reduced latency.

The trend of combining has also been researched and developed in recent years based on open source technology and ASIC technology, initially FPGA technology. Due to the high cost of ASIC technology, large quantities of production must be ensured, so most of them are small technology companies, and in the first research steps people used a combination of FPGA technology and technology. open source code. The combination of software and hardware has resulted in multifunctional product lines, capable of customizing functions by configuration.

Currently, in the world, there are many lines of specialized IP network encryption equipment of different brands for information security purposes on the network, such as systems of Cisco, Juniper, Checkpoint, Rohde&Schwarz, Crypto AG , CE-Infosys, Thales, etc. Platform VPN solutions can be based on IPSEC, SSL/TLS protocol suites or a specific set of dedicated solutions. Some typical products include:

A. Products of CE-Infosys

CE-Infosys is a German company specializing in the development of network and data security products. Its network security products are divided into two categories, one for commercial, one for government.

Government Products: These products are designed for the high security requirements of governments. These designs were designed by CE-Infosys to allow governments to customize their cryptographic algorithms, which are hard-coded on top of the FPGA. There are two product lines for government which are ANIS and Premium [2].

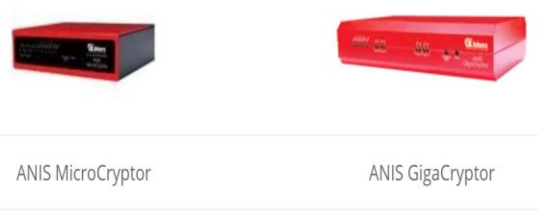


Figure 1. ANIS Micro and Giga Crypto

ANIS (Advanced Network Infrastructure) Products: ANIS products when delivered to the customer will not include software and the end user has full rights to install software and algorithms into the system or these products. will be provided with the source code to provide transparency and the customer can customize the algorithm. ANIS products include self-protection mechanisms for the system, and the plaintext and cryptotext in the ANIS product are completely separate. The cryptographic processing algorithms for IP packets, including session key generation, are implemented in the FPGA.

Figure 2. Premium Products of CE-Infosys

Premium products: Premium products do not provide self-protection for the system, all Premium products support advanced IPSec algorithm and change encryption key for each IP packet..

Commercial products: There are two product lines for Layer 2 and Layer 3, both of which use the standard AES-256 encryption algorithm and use smart card for authentication. Commercial products have two modes (Gateway and Bridge)

Gateway mode: The system acts as a router with subnets on both plain and encrypted (crypt) interfaces, the entire IP packet is encrypted and then repackaged into a new packet. . This mode supports Subnet Based Encryption (Subnet Based Encryption) ie the system works both to allow encryption and to allow explicit.

Bridge mode: Bridge mode encrypts only the payload and keeps the IP header. This technique will have advantages when used in MPLS networks. Bridge mode uses the same set of rules as Firewall, defining what to encrypt and what not to.

B. Products of TCCsecure

Cipher X 7210	Cipher X 7211
Cipher X 7220	KEYNET

Figure 3. Products of TCC secure

TCCsecure is an American security company with over 55 years of experience, its products for the field of network security include:

- Cipher X 7210: performance 100 Mb/s

- Cipher X 7211: performance from 100 to 1000 Mb/s, support for customizing algorithms.

- Cipher X 7220: performance from 1 to 10Gb/s, support for algorithm customization

All TCCsecure products [4] support Layer 2, 3, and 4 security, using GCM-mode 256-bit AES encryption. These products use a supervisory management system called KEYNET.

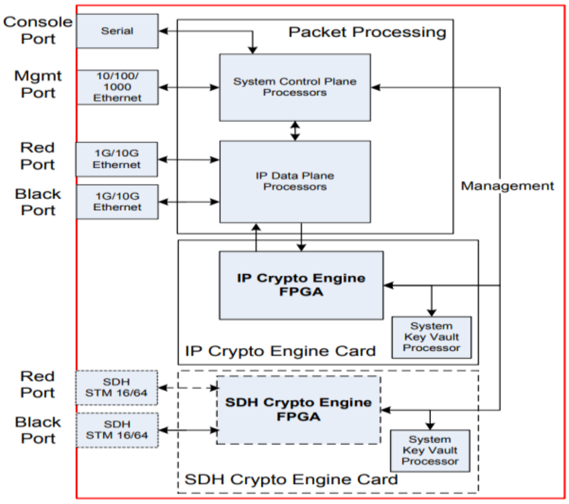


Figure 4. Motorola's Security Solution

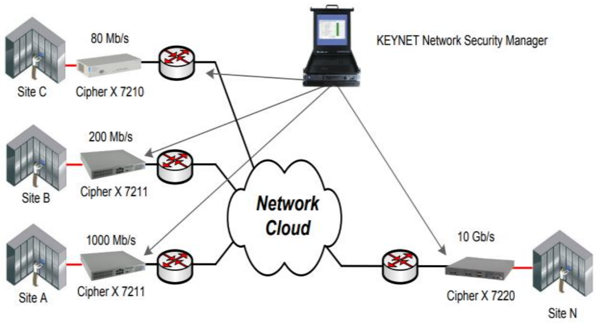


Figure 5. Security model of TCC secure

C. Products of Rohded & Schwarz

Rohded&Schwarz is a German company, its network security products are also very famous around the world. The company has Layer 2 and 3 security products, ranging from 100Mb/s to 40Gb/s bandwidth [3].

- Security product R&S®SITLine ETH: Security system at level 2.

+ Low latency (only 3us), ensuring SNMP network monitoring and management, security management center, low power consumption, bandwidth can be up to 40 Gb/s.

+ Encryption algorithm: AES-256, CFB mode, GCM, point-to-point or group encryption

+ Key exchange algorithm: ECC 257 bits

+ Certificate X509v3

- Security product R&S®SITLine IP Layer-3: Security system at layer 3.

Bandwidth up to 10 Gb/s

+ Group encryption solution

+ Latency: ≤ 10us for 10G version, ≤ 35us for 1G version, ≤ 150us for 100M version.

+ Encryption algorithm: AES-256 GCM, 8-16 byte checksum and anti-replay attack.

+ Authentication: Algorithmic signature on elliptic curve with 384-bit and 512-bit key

+ Certificate X509v3.

+ Supports SNMP v2c and v3 protocols for management and monitoring.

+ Trust management center

R&S®SITLine ETH

Ethernet Encryption HC-8552 1G Multipoint

Figure 6. Rohded&Schwarz security products

D. Products of Crypto AG

Crypto AG is a major security company in the world, providing a wide range of security solutions for both hardware and software. Particularly for network security products, the company has products from 100Mbps to 100Gb/s bandwidth, both copper and fiber interface.

Crypto Link HC-8682 100G

Ethernet Encryption HC-8552 1G Multipoint

Figure 7. Network security product of CryptoAG

Some of the company's typical products are:

- CRYPTO LINK HC-8682 100G: This is a secure system with bandwidth up to 100Gb/s with optical interface for backbone networks and large data centers. With Crypto link HC-8682 100G, data is protected at the infrastructure level without compromising higher layer service applications.

- Similar to Crypto link HC-8682 100G, the company has Ethernet security systems for lower bandwidths such as 10G, 1G, these products are transparent to user applications.

E. Products of Thales.

Figure 8. Network security products line 5000 series of Thales

Thales is a well-known American security company, for network security, Thales has the DATACRYPTO 5000 Series product line [1]. Some technical characteristics of this product line:

- Performance:

- Group key encryption (up to 1000 points)
- Real-time encryption of Ethernet packet data (Ethernet payload IEEE 802.3)
- Packet size and packet content independent encoding
- Changing the key without losing data
- Latency:
    - For 100Mbps bandwidth no more than 40us
    - For 1 Gbps bandwidth no more than 9us•

- Key management:

- Ad-hoc system authentication
- Anti-forgery key storage
- Key integration server for group key distribution
- Automatically change master key and group lock activation time.

- Encryption:

- 256-bit AES-GCM encryption algorithm
- Data integrity and anti-replay using Galois counter mode (GCM)
- Generate keys from random source using hardware
- Key exchange: Difie-Hellman ECC (DH-ECKAS)
- Meets FIPS 140-2 L3

- System management:

- Configuration via RS232 . port
- Integrated monitoring, network status and activity
- Remote monitoring via SNMP
- Monitor communication through CryptoMon software.

F. Development trend of IP network security devices

Through researching and surveying the current research situation in the world, it can be seen that some common design trends of IP network encryption systems:

- Modularity and design diversification: Most commercial IP network encryption systems for device hardware provide customers with the ability to choose from different hardware configurations, license packages Software support ensures flexibility and flexibility in deployment across different application environments. Diversity is not only reflected in the type and size of devices, but also in terms of bandwidth from low bandwidth of 100Mb/s to medium bandwidth of 1Gb/s, 10Gb/s to high bandwidth of 40Gb /s, 100Gb/s; connection interface: copper interface and optical interface; The security layer corresponds to the processing performance requirements: from layer 2, layer 3 to layer 4.

- The trend of hardening cryptographic algorithms that clearly separate the code from the clear in the design has become popular to meet the requirements of processing performance and system upgrade management.

- Development of management systems, configuration, monitoring and cyclical technical operation and maintenance services as an extension of the system: the management interfaces are implemented quite diversely, including: command line interface, web interface and proprietary management system including management server and management client.

Although some systems provide the ability to integrate algorithms according to user requirements, they are mainly based on softening, which significantly reduces the processing performance of the system. On the other hand, the security and safety of the system and the dependence on third parties both in the process of expanding, developing and upgrading the system or algorithms and deploying and using is also one of the limitations besides the cost. of the system when deployed in areas under the scope of state secrets. Therefore, the autonomous research, design, manufacture and development of domestic IP network encryption systems is one of the urgent problems.

G. Design local IP network security devices

For local IP network security devices, it must be mentioned that VGISC's IP network security devices are used in the Government and defense sectors. These devices are developed and perfected through many different versions. For devices designed on FPGA platforms the execution speed is usually below 100Mb/s. For devices designed on PowerPC platform combined with FPGA the execution speed is usually below 220Mb/s. In addition, the IPSEC VPN security products of development teams from the Institute of Electronics/Institute of Science and Military and Vietkey are carried out in the national research project KC.01.08/15. The product is built on the FPGA platform. According to the author's announcement, this product has an encoding speed of about 75 Mb/s when using 100 Mb/s Ethernet communication. The device is capable of encrypting using AES 256-bit algorithm all packets from the IP layer, protocols and upper layer services such as Web, FTP, SMTP/POP3 (Email), VoicelP, Video Conferencing, ..

In general, the developed domestic IP network encryption products have proven their feasibility in mastering the design and manufacturing technology of IP network security devices in Vietnam. The technology approach has initially approached the trends of approaching IP security technology in the world on both L2 and L3 layers on copper and fiber technology, using foundational hardware design technology. are FPGAs. The above products are capable of meeting the needs of use in systems that do not require large bandwidth and are small in scale. However, the products have many limitations not only in terms of bandwidth, the ability to ensure the number of connections, redundancy but also in terms of management, configuration, and monitoring. In particular, there are a number of product lines of cryptographic algorithms and parameters that need to be upgraded and replaced to meet new cryptographic security standards. Select and develop technology solutions that ensure optimal design, openness for development, overcome the limitations indicated, and ensure compatibility with current IP network security devices. Deployment is one of the challenges for the design of current and future IP network security devices. The hardware and software upgrade solutions presented below are described for the purpose of upgrading the bandwidth of local IP network security devices.

III. SOLUTIONS TO UPGRADE LOCAL IP NETWORK SECURITY DEVICES

In this section, the authors will present solutions to upgrade the system's hardware and software platforms, including the central security device, the terminals, and the core for advanced secure cryptography. processing performance of the system.

A. Choosing hardware design technology

Mastering design and manufacturing technology is one of the important requirements in the development of domestic security systems. Depending on the level of scientific and technological development of countries, the degree of mastery in design and manufacturing technology is at different levels. Most of the IP network security products manufactured in Russia, used in the defense sector, are based on specialized processors developed in Russia and therefore the ability to master the design technology. manufactured at a very high level. However, this is not a common trend in the development of IP network security systems and is not feasible for the domestic level of scientific and technological development in the country. Therefore, the selection of technology platforms is one of the first basic requirements in the design. Currently, many chip lines are commercialized on PowerPC/ARM/FPGA platforms of high-configuration companies around the world, suitable for designing high-speed IP network security products such as: QorIQ T series, NXP's P series, Zynq SoC, Zynq Ultrascale, Zynq Ultrascale+, Kintex series, Xilinx's Virtex, IMX6, IMX8 by NXP...with support for DDR3 ram memory up to 24GB, DDR4 up to 24GB, high-speed interfaces such as USB3 .0, PCIe Gen2, PCIe Gen3, Tri mode Gigabit Ethernet, high speed transceivers.... However, designing the hardware for these chips is extremely difficult and complex. Usually, in terms of using software, there will be a lot of support from the company as well as on the internet, for hardware companies will have development kits and design samples, but to have a product, we have to design it ourselves. designs based on these sample designs. This is a job that requires a lot of effort and expense. We will look at several design options for IP network security devices to improve their speed and bandwidth.

1. Solutions for designing IP network security devices in Gateway mode

a. Solution 1:

Using PowerPC chip combined with Kintex FPGA chip, in which PowerPC chip will handle software to increase system flexibility, and FPGA chip plays the role of processing chip to speed up encryption algorithms and increase security. for the system. The block diagram of the design is as shown below.

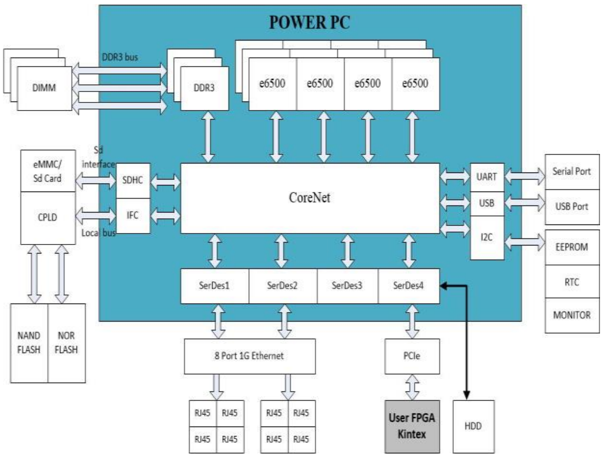


Figure 9. Block diagram of IP network security device design in Gateway mode, the option to combine FPGA and Power PC technology

For this option, in addition to studying the design of hardware and software on two chip lines, PowerPC and Kintex, the problem of designing high-speed communication between PowerPC and Kintex is also complicated and requires implementation.

b. Solution 2

Using System on chip Zynq, Zynq ultrascale or Zynq ultrascale+ of Xilinx, this is a multi-core chip that integrates both FPGA and ARM cortex A53 on one chip, very convenient for design. The proposed block diagram is as shown below:

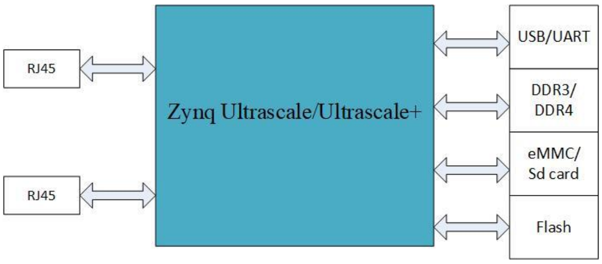


Figure 10. Block diagram of the Gateway mode IP network security device design using FPGA technology integrated with ARM platform

Of these two solutions, each has its own advantages and disadvantages.

For solution 1: can use 64-bit PowerPC e6500 chip as PowerPC, this is a chip line manufactured on 28 nm technology. The advantage of this option is the chip's powerful processor with 24 virtual cores, 1.8Ghz CPU speed, support for DDR3 up to 24GB, 8 1 Gigabit Ethernet ports, 4 10G SFP ports, which are very suitable for the development of mobile applications. high speed network equipment. The difficulty is that for a specialized security device that requires hard encryption, an additional FPGA chip is required to handle the hardening of the external encryption algorithm.

For solution 2: to have the same processing performance as the PowerPC e6500 can use Xilinx's Zynq ultrascale+ chip line, a very new and powerful chip of the SoC platform manufactured on 16 nm technology. The advantage of this option is the flexible combination of FPGA and ARM on a single chip. ARM part can choose dual-core, quad-core Cortex-A53, chip supports DDR3, DDR4, CPU speed 1.5Ghz, 4 Tri-mode Gigabit Ethernet. With this chip, users can combine software (ARM) handling the IP Stack and FPGA processing hardening encryption algorithms on the same chip. However, this option also encounters many difficulties, that is, with 16 nm technology, the design and manufacture of hardware is very complicated, in the country today, there are few units capable of mastering the hardware design of the company. this chip. Moreover, the cost of FAB board is very expensive, in addition, it is very difficult to expand the number of Ethernet ports.

Therefore, the authors follow the direction of using solution 1 to design and manufacture a high-speed IP network security device in Gateway mode.

2. *Bridge mode IP network security device design solution*

I. For Bridge mode IP network security device, because it does not have to deal with complicated packet routing like in Gateway mode, it is not necessary to integrate the operating system on the device. Therefore, the authors aim to use the FPGA chip to perform Ethernet packet extraction and encryption to optimize bandwidth for the device. To ensure the feasibility of designing the author's team using Xilinx's Zynq 7000 chip, this is a relatively suitable SoC chip for the design of Bridge mode central IP network security devices.

Proposed block diagram:

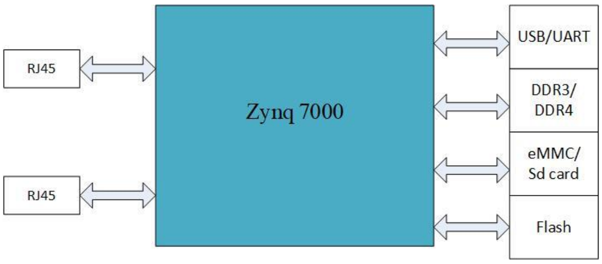


Figure 11. Bridge mode IP network security device design block diagram using FPGA . technology

IV. SOME RESULTS OF SIMULATION AND DESIGN IMPLEMENTATION

A. Realize high-speed communication between PowerPC and FPGA in Gateway mode IP network security appliance

Hardware Specifications

- Board PowerPC: Chíp T4240, 16GB, DDR3, PCIe Gen2x8

- Card PCIe Gen2 x8: Chip Kintex 7 XC7K325TFFG676-2.

For communication between PowerPC and FPGA use the PCIe DMA Gen2 x8 interface.

a. Implement PCIe communication between PowerPC and FPGA without built-in encryption algorithm

To implement communication between PowerPC and FPGA via PCIe interface, we use IP core DMA/Subsytem in Xilinx's Vivado with the following basic parameters: PCIe Gen2 x8, DMA Memory map mode, Poll mode. Design block diagram as shown below:

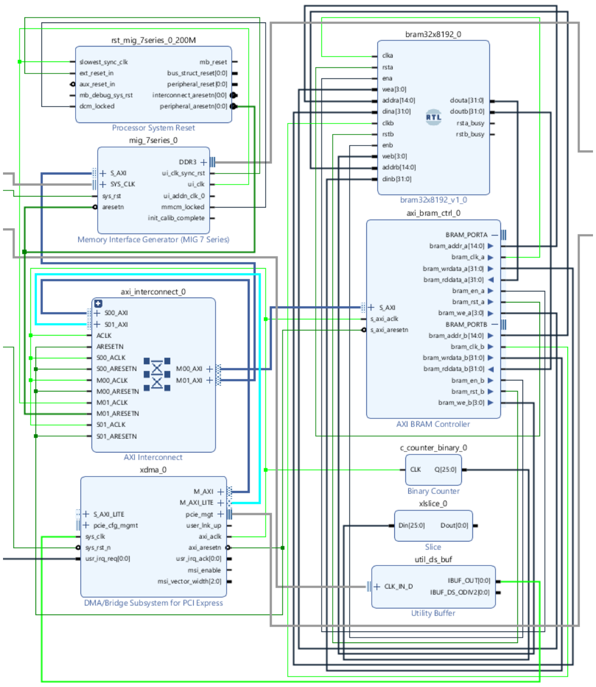
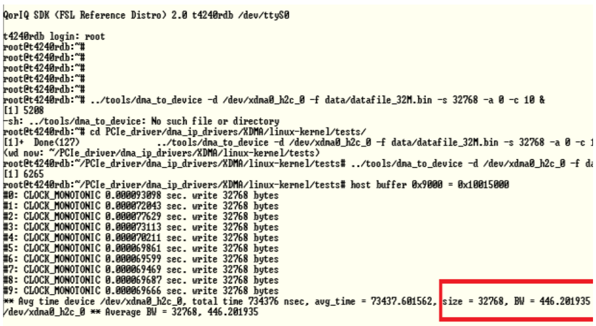


Figure 12. PCIe DMA interface design block diagram on FPGAs without built-in encryption

Bandwidth measurement results:



```
QorIQ SDK (FSL Reference Distro) 2.0 t4240rdb /dev/ttyS0

t4240rdb login: root
root@t4240rdb:~#
root@t4240rdb:~#
root@t4240rdb:~#
root@t4240rdb:~#
root@t4240rdb:~#
root@t4240rdb:~# ../tools/dma_to_device -d /dev/xdma0_h2c_0 -f data/datafile_32M.bin -s 32768 -a 0 -c 10 &
[1] 5208
-sh: ../tools/dma_to_device: No such file or directory
root@t4240rdb:~# cd PCIe_driver/dma_ip_drivers/XDMA/linux-kernel/tests/
[1]+  Done(127)              ../tools/dma_to_device -d /dev/xdma0_h2c_0 -f data/datafile_32M.bin -s 32768 -a 0 -c 1
(wd now: ~/PCIe_driver/dma_ip_drivers/XDMA/linux-kernel/tests)
root@t4240rdb:~/PCIe_driver/dma_ip_drivers/XDMA/linux-kernel/tests# ../tools/dma_to_device -d /dev/xdma0_h2c_0 -f da
[1] 6265
root@t4240rdb:~/PCIe_driver/dma_ip_drivers/XDMA/linux-kernel/tests# host buffer 0x9000 = 0x10015000
#0: CLOCK_MONOTONIC 0.000093098 sec. write 32768 bytes
#1: CLOCK_MONOTONIC 0.000072043 sec. write 32768 bytes
#2: CLOCK_MONOTONIC 0.000077629 sec. write 32768 bytes
#3: CLOCK_MONOTONIC 0.000073113 sec. write 32768 bytes
#4: CLOCK_MONOTONIC 0.000070211 sec. write 32768 bytes
#5: CLOCK_MONOTONIC 0.000069861 sec. write 32768 bytes
#6: CLOCK_MONOTONIC 0.000069599 sec. write 32768 bytes
#7: CLOCK_MONOTONIC 0.000069469 sec. write 32768 bytes
#8: CLOCK_MONOTONIC 0.000069687 sec. write 32768 bytes
#9: CLOCK_MONOTONIC 0.000069666 sec. write 32768 bytes
** Avg time device /dev/xdma0_h2c_0, total time 734376 nsec, avg_time = 73437.601562, size = 32768, BW = 446.201935
/dev/xdma0_h2c_0 ** Average BW = 32768, 446.201935
```

Figure 13. Unencrypted Gateway mode IP network security device bandwidth test results

The actual results measured on the T4240 board and the PCIe Kintex 7 board we designed are 446.2 MB/s when transmitting data with a buffer of 32768 bytes per channel, when using 2 channels at the same time, the speed will be multiplied by 2.

b. Implement PCIe communication between PowerPC and FPGA with built-in encryption algorithm

Design block diagram on FPGA as shown below:

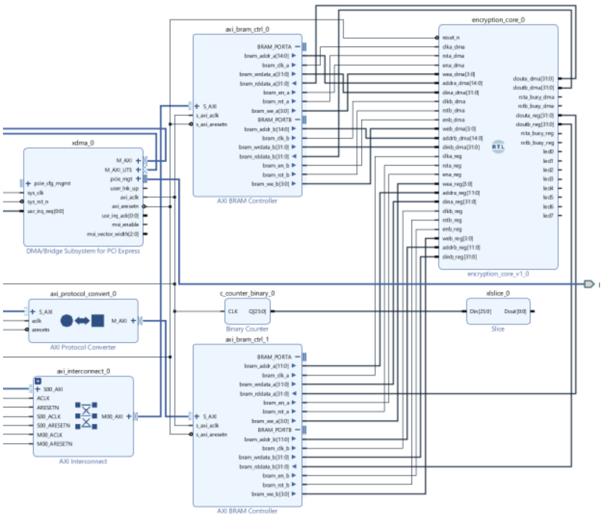
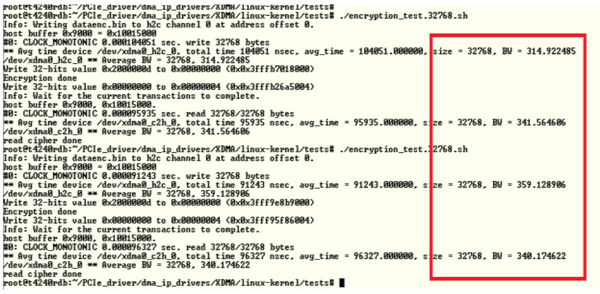


Figure 14. PCIe DMA interface design block diagram on FPGA with built-in encryption

In this design we use 2 independent memory areas, one area for control communication, lock, IV, one memory area for data communication.

Bandwidth measurement results:

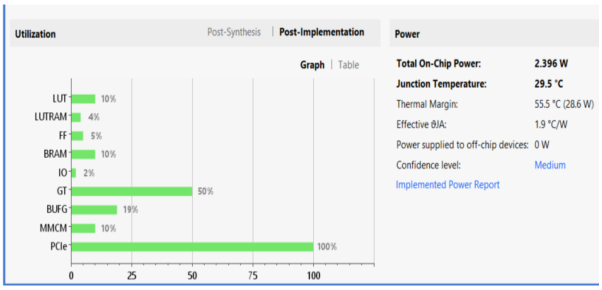


```
root@t4240rdb:~/PCIe_driver/dma_ip_drivers/XDMA/linux-kernel/tests#
root@t4240rdb:~/PCIe_driver/dma_ip_drivers/XDMA/linux-kernel/tests# ./encryption_test.32768.sh
Info: Writing dataenc.bin to h2c channel 0 at address offset 0.
host buffer 0x9000 = 0x10015000
#0: CLOCK_MONOTONIC 0.000104051 sec. write 32768 bytes
** Avg time device /dev/xdma0_h2c_0, total time 104051 nsec, avg_time = 104051.000000, size = 32768, BW = 314.922485
/dev/xdma0_h2c_0 ** Average BW = 32768, 314.922485
Write 32-bits value 0x2000000d to 0x00000000 (0x0x3fffb7018000)
Encryption done
Write 32-bits value 0x00000000 to 0x00000004 (0x0x3fffb26a5004)
Info: Wait for the current transactions to complete.
host buffer 0x9000, 0x10015000.
#0: CLOCK_MONOTONIC 0.000095935 sec. read 32768/32768 bytes
** Avg time device /dev/xdma0_c2h_0, total time 95935 nsec, avg_time = 95935.000000, size = 32768, BW = 341.564606
/dev/xdma0_c2h_0 ** Average BW = 32768, 341.564606
read cipher done
root@t4240rdb:~/PCIe_driver/dma_ip_drivers/XDMA/linux-kernel/tests# ./encryption_test.32768.sh
Info: Writing dataenc.bin to h2c channel 0 at address offset 0.
host buffer 0x9000 = 0x10015000
#0: CLOCK_MONOTONIC 0.000091243 sec. write 32768 bytes
** Avg time device /dev/xdma0_h2c_0, total time 91243 nsec, avg_time = 91243.000000, size = 32768, BW = 359.128906
/dev/xdma0_h2c_0 ** Average BW = 32768, 359.128906
Write 32-bits value 0x2000000d to 0x00000000 (0x0x3fff9e8b9000)
Encryption done
Write 32-bits value 0x00000000 to 0x00000004 (0x0x3fff95f86004)
Info: Wait for the current transactions to complete.
host buffer 0x9000, 0x10015000.
#0: CLOCK_MONOTONIC 0.000096327 sec. read 32768/32768 bytes
** Avg time device /dev/xdma0_c2h_0, total time 96327 nsec, avg_time = 96327.000000, size = 32768, BW = 340.174622
/dev/xdma0_c2h_0 ** Average BW = 32768, 340.174622
read cipher done
root@t4240rdb:~/PCIe_driver/dma_ip_drivers/XDMA/linux-kernel/tests# █
```

Figure 15. Bandwidth test results of Gateway mode IP network security devices with code

The actual results we measured on the T4240 board and the PCIe Kintex 7 board we designed are about 340 MB/s when transmitting encrypted data with a buffer of 32768 bytes per channel.

Parameters of resources used on the XC7K325TFFG676-2 chip



Power

Total On-Chip Power: 2.396 W
Junction Temperature: 29.5 °C
Thermal Margin: 55.5 °C (28.6 W)
Effective ϑJA: 1.9 °C/W
Power supplied to off-chip devices: 0 W
Confidence level: Medium
Implemented Power Report

Figure 16. Resources used on the XC7K325TFFG676-2

B. Bridge-mode IP network security device design implementation

The board is designed on Xilinx zynq 7000 XC7Z020CLG484-1 microprocessor chip. For this design, we do completely IP data extraction and encryption on the same FPGA chip. Where the block diagram is designed to separate the packet processing area and the encryption area, the block diagram is designed as shown below:

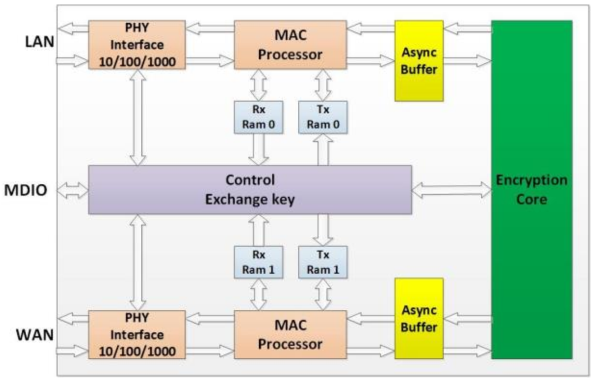
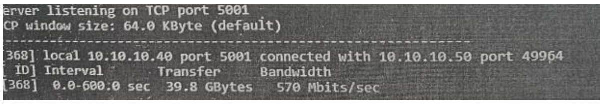


Figure 17. Block diagram of Bridge mode encryption and packet fragmentation implementation

In this design, we completely use the chip's logic elements in the design, do not use any ip core of the company, so it is easy to change the choice of chip line.

The resulting bandwidth we measured between 2 Bridge mode encoders between 2 computers is 570 Mbits/s.



```
erver listening on TCP port 5001
CP window size: 64.0 KByte (default)
------------------------------------------------------------
368] local 10.10.10.40 port 5001 connected with 10.10.10.50 port 49964
 ID] Interval       Transfer     Bandwidth
[368]  0.0-600.0 sec  39.8 GBytes   570 Mbits/sec
```

The proposed solution has been applied in the design and manufacture of IP network security devices upgraded version 2022 and demonstrates its superiority in bandwidth compared to other local product lines.

This result can completely improve the speed when replacing more powerful chips like XC7Z030 or XC7Z045 of Xilinx.

V. CONCLUTION

In this study, on the basis of research on technological solutions in the design and manufacture of IP network security systems in the world, the authors have synthesized and given their development trends, combining with discussing the challenges posed to domestic IP network security systems, propose solutions to upgrade, design, and manufacture to ensure optimality based on the combination of PowerPC and FPGA hardware technology.

The proposed solution has been applied in the design and manufacture of a number of IP network security product lines in practice. The simulation and experimental data are executed with 1GB communication port without authentication.

Experimentally, the authors have proven the effectiveness of the proposed solution, the IP network security devices after the upgrade ensure stability in operation, and the post-upgrade speed is superior to previous versions.

ACKNOWLEDGMENT

The authors would like to express their sincere thanks to the valuable comments of the reviewers the suggestions, and the support from the Institute of Cryptographic Science and Technology and the M2 factory at VGISC.

REFERENCES

[1]. Thalesgroup.com. “Thales delivers high performance, low latency data protection for data in transit” Available: https://www.thalesgroup.com/en/datacryptorr-sonet November. 25, 2015. [Accessed: February.10, 2022]

[2]. Ce-infosys.com “ANIS microcryptor” Available: https://www.yumpu.com/en/document/read/2627906/anis-microcryptor-ce-infosys-gmbh March. 20, 2022. [Accessed: March. 20, 2022]

[3]. Rohde-schwarz.com “Secure ethernet encryption via landline, radio relay and satellite links up to 40 Gbit/s” Available: https://www.rohde-schwarz.com/uk/products/cybersecurity/network-encryptors January. 20, 2022. [Accessed: January. 20, 2022]

[4]. Tccsecure.com “Cipherx 7220M” Available: https://www.tccsecure.com/Products/network-encryption/cipherx7220M-detail.aspx March. 20, 2022. [Accessed: March. 20, 2022]

ABOUT THE AUTHORS

Tran Van Khanh

Workplace: Department of Science and Technology of VGISC.

Email: trankhanh.miptvn@gmail.com

Education: He received his Radio Engineering and Cybernetics Bachelor’s degree in 2009, his master’s degree Electronic Computers, Computer Engineering in 2011, and his PhD in System analysis, control and information processing at Moscow Institute of Physics and Technology.

Recent research direction: Cryptographic techniques; research, design and manufacture a dedicated security system based on ASIC and FPGA.

Nguyen Van Tu

Workplace: M 2 of VGISC

Email: tunguyenm2@gmail.com

Education: He received his in Cryptographic Techniques Bachelor’s degree in 2005, his master’s degree in Cryptographic techniques in 2014 at Academy of Cryptographic Techniques

Recent research direction: Cryptographic Techniques; research, design and manufacture a dedicated security system based on ASIC and FPGA.

Truong Phi Ho

Workplace: Telecommunications University

Email: phihosqtt@gmail.com

Education: Master of Sciences

Recent research direction: cyptography, privacy – preserving datamining and machine learning.