情報保護學會論文誌
第15卷 第5號, 2005. 10

네트워크 환경에 적합한 AES 암호프로세서 구조 분석*

윤 연 상,[1†] 조 광 두,[1] 김 용 대,[1‡] 한 선 경,[2] 유 영 갑[1]
[1]충북대학교 정보통신공학과, [2]특허청

Structure Analysis of AES Cryptoprocessor based on Network Environment*

Yeonsang Yun,[1†] Kwangdoo Jo,[1] Yongdae Kim,[1‡]
Seonkyoung Han[2] and Younggap You[1]
[1]Dept. of Information and Communication Engineering, Chungbuk Nat'l University,
[2]The Korea Intelligent Property Office

요 약

본 논문은 AES 암호프로세서의 성능분석모델을 제안하였다. 제안된 모델은 M/M/1 큐잉 모델을 기반으로 포아송 분포를 트래픽 입력으로 가정하였다. 모델을 이용한 성능분석결과 1kbyte 패킷입력에서 AES 암호화 10라운드를 1클록에 처리하게끔 설계된 파이프라인 구조가 10클록에 처리되는 비-파이프라인 구조에 비하여 4.0% 정도의 성능향상만을 확인하였다. FPGA상에서 AES 암호프로세서를 구현한 결과 파이프라인 구조는 비-파이프라인 구조와 비교하여 게이트 수는 3.5배 크게 소요되었으나 성능은 3.5%의 증가만을 나타내었다. 제안된 모델은 네트워크 컴퓨터에 사용될 AES 암호프로세서 설계 시, 최적의 가격대성능비를 갖는 구조를 제시할 수 있을 것으로 기대된다.

ABSTRACT

This paper presents a performance analysis model based on an M/M/1 queue and Poisson distribution of input data traffic. The simulation on a pipelined AES system with processing rate of 10 rounds per clock shows 4.0% higher performance than a non-pipelined version consuming 10 clocks per transaction. Physical implementation of pipelined AES with FPGA takes 3.5 times bigger gate counts than the non-pipelined version whereas the pipelined version yields only 3.5% performance enhancement. The proposed analysis model can be used to optimize cost-performance of AES hardware designs.

Keywords : *AES, Cryptoprocessor, Performance Analysis*

Ⅰ. 서 론

네트워크상의 보안의 중요성이 제기되면서 SSL이나 IPSec 프로토콜과 같은 보안 어플리케이션이 개발되어왔다. 이러한 프로토콜들은 주로 통신 양단간의 상호 인증을 토대로 주요 데이터를 암호화함으로써 보안 공격에 대응하고 있다. 이미 운영체제의 선두에 있는 마이크로소프트사의 Windows 계열은 IPSec 프로토콜의 사용을 일반화하고 있다. 운영체제와 같이 소프트웨어 상에서 암호관련 연산을 수행할 경우 CPU는 상당한 연산을 처리해야 한다. 실제로 최근의 연구결과에 의하면 암호관련 연산 수행 시 지속적으로 95% 정도의 CPU 자원을 소모한다고 밝히고 있다.[1] 이러한 문제점을 극복하기 위한 방안으로 암호연산을 대신 처리하는 암호프로세서가

접수일 : 2004년 1월 5일 ; 채택일 : 2005년 7월 11일
* 본 연구는 산업자원부의 지역혁신 인력양성사업의 연구결과이다.
† 주저자, ysyun@hbt.chungbuk.ac.kr
‡ 교신저자, ydkim@hbt.chungbuk.ac.kr

연구되고 있다.[2]

IPSec이나 SSL 기능이 내장된 암호엔진(Crypto-engine) 형태의 프로세서들은 단순히 암호 모듈의 성능향상이 아닌 사용될 시스템에 적합하도록 설계방향을 결정해야 한다. 암호프로세서를 이용한 IPSec/SSL 가속장치들은 이미 상용화되고 있다.[3,4] 이 제품들은 보안서버등과 같은 네트워크 컴퓨터에 장착될 수 있도록 PCI 인터페이스를 지원한다. 구체적으로 가속장치내부의 암호프로세서로부터 처리된 연산의 결과들은 모두 PCI를 통해 네트워크 컴퓨터의 메모리에 저장된다. 암호프로세서의 처리율은 PCI의 전송률의 영향을 받는다. 예를 들어, 10Gbps의 처리속도를 갖는 AES 블록암호 모듈은 연산결과를 실시간으로 메모리에 저장할 수 없다. PCI 64bit, 66MHz 규격의 경우 최대 4.2Gbps의 데이터전송까지 가능하기 때문이다. 패킷크기에 따른 디코딩 지연은 IPSec/SSL가속장치와 PCI 간의 오버헤드와 마찬가지로 암호프로세서의 고속처리능력을 무력화시키는 원인이다. 현재 네트워크 트래픽의 경우 대부분 1kbyte 미만의 패킷크기를 갖는다.[5] 패킷은 헤더를 포함하는 최소단위로 단대단 데이터처리를 위한 경계이다. 같은 크기의 파일을 수신할 경우라면, 1Mbyte와 1kbyte 패킷을 컴퓨터가 처리하기 위해 패킷헤더를 디코딩하는 회수가 전자에 비해 후자가 1000배 많다. 디코딩과정은 OS와 어플리케이션과 같은 소프트웨어의 처리를 요하기 때문에 하드웨어인 암호프로세서와 비교하여 상당히 저속으로 진행될 수밖에 없다.

암호프로세서는 단일 칩 안에 AES 또는 DES 등의 블록 암호 모듈과 ECC나 RSA 등의 공개키 암호 모듈이 탑재된다. 단일 칩 암호프로세서의 모듈에 따른 하드웨어 면적을 그림 1에서 나타내었다.[6] 본 논문에서는 칩 전체면적에 대하여 각각의 암호모듈들이 차지하는 면적을 백분율(%)한 결과를 소비율로 정의하였다. 본 예시에서 AES의 경우 약 390Mbit/s 정도의 암호화 연산을 수행하게끔 설계되었다.[6] 만약 AES의 파이프라인을 확대하여 780 Mbit/s의 성능과 26%의 하드웨어 소비율로 증가시켰을 경우 네트워크 컴퓨터상에서 2배의 성능 증가를 가져오는지는 장담할 수 없다. 따라서 네트워크 컴퓨터에서의 사용을 목적으로 제작되는 암호프로세서들은 그 설계 이전에 네트워크 컴퓨터에 장착되었을 경우의 성능분석이 필수적이다. 성능분석을 통해 암호프로세서가 네트워크 입력을 처리하기 위해 요구되는 최소성능을 계산할 수 있으며 과도한 파이프라인 구조로 인해 불필요하게 하드웨어 면적을 낭비하고 있는지 여부를 판별할 수 있다. 본 논문에서는 최적의 성능을 갖는 AES 암호프로세서의 구조를 평가하기 위하여 이를 네트워크 컴퓨터에 장착한 경우의 성능분석 모델을 제안한다. 제안하는 암호프로세서는 M/M/1 큐잉 시스템기반으로 모델링되었으며 네트워크상의 입력트래픽으로는 포아송분포를 가정하였다.[8]

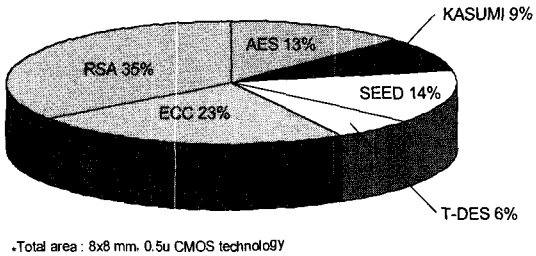


그림 1. 단일 칩 암호프로세서의 하드웨어 소비율[6]

논문의 구성은 다음과 같다. Ⅱ장은 AES 암호프로세서의 성능분석 모델을 제안하였다. Ⅲ장은 제안된 모델을 이용하여 AES의 하드웨어 구조에 따른 성능을 분석하였다. PCI기반 FPGA 에뮬레이터를 이용한 구현 결과를 바탕으로 AES의 하드웨어 구조에 따른 성능을 분석한 뒤 모델링의 결과와 비교하였다. Ⅳ장에서는 본 논문의 결론을 맺었다.

Ⅱ. AES 암호프로세서 성능분석 모델

본 절에서는 네트워크 컴퓨터에 탑재된 암호프로세서의 성능을 분석하여 성능저하의 원인을 파악하였다. 성능저하의 원인을 디코딩지연으로 정의하였으며 이 값을 구체적으로 산출하는 과정을 설명한다. 그리고 제안된 성능분석 모델을 기반으로 디코딩지연을 포함한 시뮬레이션 방법을 제시하였다.

2.1 관련연구

네트워크 컴퓨터에 장착될 경우, 실제 보안 어플리케이션의 처리시간은 암호프로세서의 처리시간 외에 운영체제 또는 컴퓨터 하드웨어의 지연시간을 포함한다. 일례로 Broadcom 사의 BCM5820의 경우 3DES+SHA 연산 시 최대 300Mbit/s의 성능을 보인다고 발표되었다.[3] 실제로 BCM5820를 네트워크 컴퓨터에 장착하여 성능을 측정하였을 경우

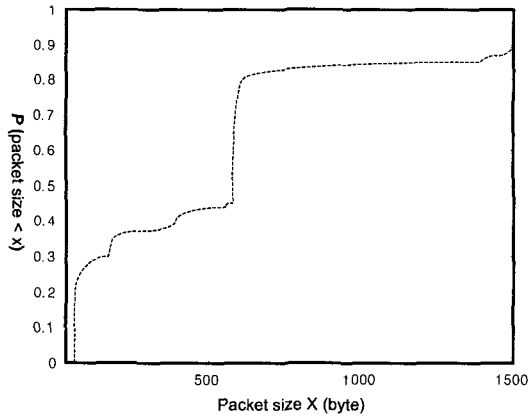


그림 2.네트워크상의 패킷분포[5]

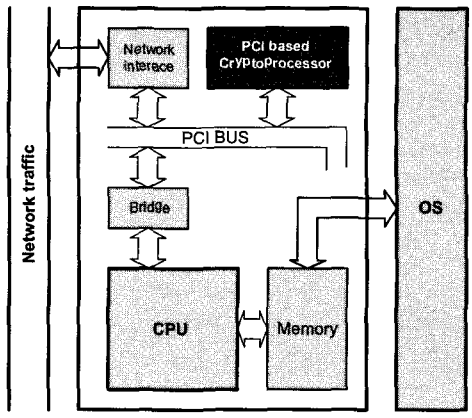


그림 3. 암호프로세서가 장착된 네트워크 컴퓨터 모형[3]

50% 정도의 성능만을 얻을 수 있는 것으로 알려졌다.[7] 50%의 성능은 크기가 64byte부터 65,535 byte 패킷까지 변화시켜가며 측정한 평균값이다. 크기가 1kbyte인 패킷의 경우 BCM5820의 10% 미만의 성능만이 확인되었다.

현재 네트워크 측정결과를 그림 2에 나타내었다. 측정결과에 따르면 당시 네트워크상에서 1500byte 이내(packet size<1500)의 패킷들이 90%정도를 차지하고 있다(2003년 기준). 1,000byte 크기 이내의 패킷들은 80%정도 분포되어 있음을 확인할 수 있다. 따라서 BCM5820과 같은 가속장치들은 실제 네트워크에서는 자신의 능력에 비해 낮은 성능을 보일 것으로 판단된다. 이렇게 성능이 낭비되는 이유는 암호프로세서가 사용될 시스템의 분석 없이 설계되었기 때문이다. 만약 암호프로세서의 설계에 전에 시스템에 장착될 경우의 성능분석이 가능하다면, 암호프로세서의 하드웨어 낭비를 줄이고 최적의 성능을 유지할 수 있을 것이다.

2.2 성능분석 모델 제안

현재 상용되는 암호프로세서들은 PCI 인터페이스를 통해 네트워크 컴퓨터에 부착된다. 이 경우의 네트워크 컴퓨터 내부 시스템은 그림 3과 같다.[3] CPU는 메모리로부터 명령을 패치한 뒤 해당 명령을 처리하게 된다. 운영체제(OS)는 메모리에서 어떠한 코드를 CPU로 넘겨줄 것인지를 결정한다. 암호프로세서의 연산기능을 사용하기 위해서는 운영체제와 메모리 그리고 CPU 등의 도움을 받아야 한다. 암호프로세서를 장착한 네트워크 컴퓨터의 모델

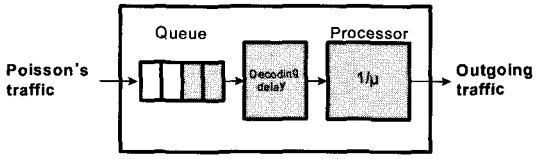


그림 4. 암호프로세서가 장착된 네트워크 컴퓨터의 큐잉모델

링을 위해서는 암호프로세서의 성능뿐만 아니라 네트워크 컴퓨터 구성요소들도 별도의 파라미터로 정의되어야 한다.

암호프로세서를 장착한 시스템을 M/M/1 시스템으로 모델링한 결과를 그림 4에서 나타내었다. 모델링을 통한 분석과정에서 실제 네트워크 트래픽 입력은 포아송 분포를 갖는 것으로 보았다. 제안된 M/M/1 시스템의 큐(queue)는 트래픽 로드를 입력받는 부분에 배치하였다. 암호프로세서는 M/M/1 시스템에서 1/μ의 처리시간을 갖는 프로세서로 대체하였다. 그 밖의 PCI버스, CPU, 메모리, 운영체제 등 네트워크 트래픽의 입력부터 암호프로세서까지 데이터를 이동시키는 경로들은 하나의 통합된 파라미터인 디코딩 지연(decoding delay)으로 정의하였다. 네트워크 모델링을 위한 구성요소의 파라미터를 표 1과 같이 정리하였다.

네트워크로부터 패킷이 입력되어 IPSec 가속기까지 연산명령이 전달되는 과정을 그림 5에서 나타냈었다. 디코딩지연(decoding delay)은 네트워크 컴퓨터에 암호프로세서를 장착했을 경우, 패킷이 프로세서까지 전달되는 경로에서의 총 지연시간을 의미한다. 디코딩지연의 손쉬운 측정을 위해 테스트 경로를 정의하였다. 간단한 TCP/IP 응용 프로그램을 통해 테스트 경로를 따라 외부로부터 입력된 패

표 1. 네트워크 모델링을 위한 구성요소의 파라미터

	네트워크 컴퓨터		모델링 파라미터	
입력	네트워크 대역폭	2500 packets/s	포아송 분포	λ = 0.4 msec
H/W	CPU	1GHz Intel P3 processor	디코딩 지연	0.5msec (그림. 8)
	Memory	256MB PC133 SDRAM		
	Hard disk	40GB WDP IDE		
	NIC	Intel PRO/1000F		
S/W	OS	Windows2000		

킷을 네트워크 컴퓨터의 메모리에 저장한 뒤 다시 외부 네트워크로 전송하기까지의 시간을 측정할 수 있다. 디코딩 경로와 테스트 경로의 경로차이가 동일함으로 테스트 경로를 거쳐 측정된 시간은 디코딩 지연과 같다.

테스트 경로를 거쳐 모든 패킷이 처리되는 총 시간을 latency라고 정의하였다. Latency는 식 2.2로부터 식 2.2를 이용하여 식 2.2와 같이 디코딩지연을 계산할 수 있다. DATA_TRANSFER_TIME은 LAN PCI 인터페이스와 같은 네트워크 인터페이스 카드(NIC)가 총 입력 데이터를 처리하는 데 걸리는 시간을 의미한다.

$$DATA\_TRANSFER\_TIME = \frac{TOTAL\_INPUT\_SIZE}{NETWORK\_INTERFACE\_BW}(sec) \quad (식\ 2.1)$$

$$Latency = (DECODING\_DELAY \times \#\ of\ packets) + DATA\_TRANSFER\_TIME\ (sec) \quad (식\ 2.2)$$

제안된 모델링을 이용한 성능과 실측성능과의 비교를 위해 표 1과 같이 Miltchev가 사용한 네트워크 컴퓨터와 비슷한 사양에서 디코딩지연 값을 관측하였다.[7] 테스트 환경에서의 TOTAL_INPUT_SIZE는 67Mbit 이고 NETWORK_INTERFACE_BW는 10Mbit/s이다. 식 2.1에 의해 NIC의 DATA_TRANSFER_TIME은 6.7초이다. 데이터의 전송을 완료하기까지 걸린 총 시간(latency)을 측정하기 위해 그림 6과 같이 TCP/IP 소켓 프로그램을 제작하였다. 본 프로그램은 클라이언트와 서버간의 파일을 전송하며 이때의 시간을 측정하도록 제작되었다. 패킷 크기를 64, 128, … , 1,024까지 증가시켰을 경우 각각의 latency를 측정한 결과를 그림 7의 그래프에서 나타내었다. 이 결과와 DATA_TRANSFER_TIME을 식 2.2에 대입하여 디코딩 지연을 계산한 결과는 그림 8의 그래프와 같다. 패킷 크기에 따른 디코딩지연 값들을 평균하여 0.5 msec의 파라미터 값을 얻었다.

Ⅲ. AES 성능분석 모델의 검증

본 절은 모델을 이용한 AES 암호프로세서의 성능분석결과와 하드웨어로 설계하여 측정된 결과와의 비교를 다루었다. 성능분석모델의 타당성을 증명하기 위해 실제 네트워크 가속장치를 대체할 수 있는 PCI 기반 FPGA 에뮬레이터를 이용하여 비파이프라인-AES와 파이프라인-AES의 성능차이를 분석하고 이를 모델링을 통한 분석결과와 비교하였다.

3.1 구현을 통한 AES 암호프로세서의 성능분석

AES의 하드웨어 구조는 그 구현방식에 따라 파

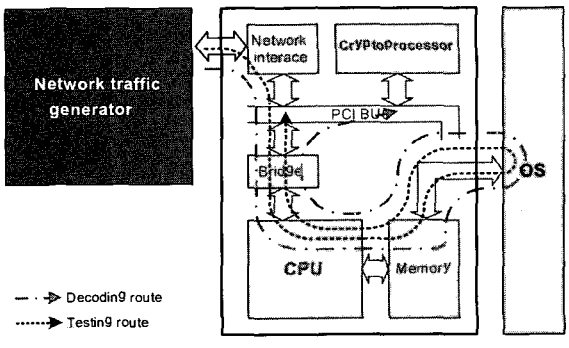


그림 5. 디코딩 경로와 테스트 경로

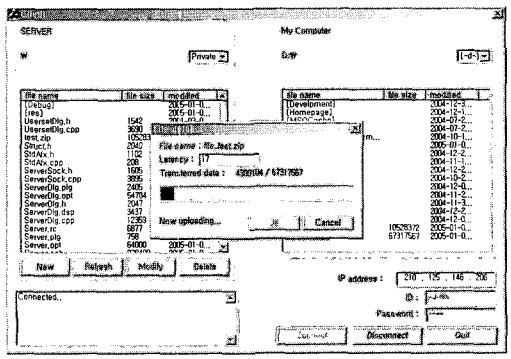


그림 6. 총 시간(latency)을 측정하기 위한 테스트 프로그램

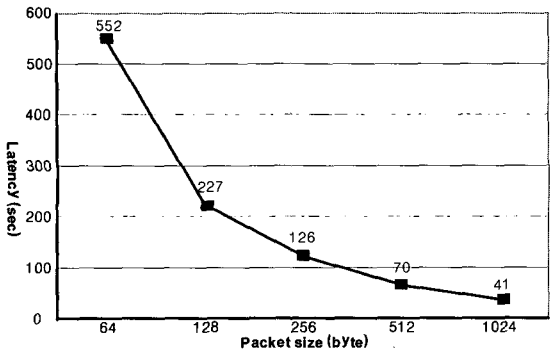


그림 7. 테스트 경로를 통해 측정된 latency

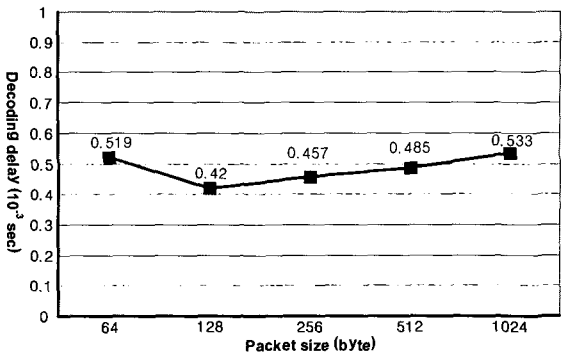


그림 8. 패킷크기에 따른 디코딩지연

이프라인 구조와 비-파이프라인 구조로 나뉜다. 비-파이프라인 구조는 FIPS-197에 명시되어 있는 AES 표준을 그대로 하드웨어로 구현하였을 경우이며 적은 게이트 수를 필요로 한다.[11,12] 반면 파이프라인 구조는 비-파이프라인 구조의 루프를 없애고 라운드에 이용되는 블록들을 모두 설계하므로 상대적으로 많은 게이트 수를 소요한다.[13]

성능분석모델의 제약사항은 다음과 같다. 우선, 암호프로세서는 네트워크 컴퓨터 상에서 PCI 인터페이스로 결합되는 구조를 같는다. CPU에 'tightly-coupled coprocessor'로 사용되는 구조는 본 성능분석 모델에서 고려하지 않았다. 본 성능분석모델의 네트워크 환경은 TCP/IP 프로토콜에서 AES 블록암호만 사용했을 경우이다. IPSec의 AH나 ESP 프로토콜에서 적용되는 해쉬나 공개키 암호등의 기능은 본 성능분석모델에 포함되지 않는다. 세 번째 제약조건으로 AES 암호프로세서의 입력데이터와 키의 길이가 128 비트일 때에만 고려한다. AES 암호화와 복호화 시 성능은 같다고 가정하였다. 일반적으로 복호화 시 모듈로 곱셈으로 인한 최장지연경로(critical path)가 크지만, 제안된 성능분석은 33 MHz의 저속 동작을 기준으로 성능을 측정하였기 때문에 최장지연경로가 암호화 및 복호화의 성능에 크게 영향을 미치지 않을 것으로 판단된다. 마지막으로 키 스케줄링 때문에 암호화 또는 복호화 라운드 외에 별도의 클록이 사용되지 않음을 가정하였다.

제안된 모델을 이용한 성능분석 결과가 실제 하드웨어로 구현된 AES 암호프로세서에서 유사한 결과를 나타내는지 확인하였다. 본 절에서는 앞선 성능분석 모델과 같은 구조의 Gbit/s급 AES 프로세서와 100Mbit/s급 AES 프로세서를 테스트 목적으로 제작하여 실제 네트워크 컴퓨터에 장착한 뒤 성능을 측정하였다. 이 두 회로는 파이프라인 구조채택 여부에 따라 다르게 설계되었다. AES의 하드웨어 구현 시, 최소의 면적을 필요로 하는 비-파이프라인구조를 그림 9와 같다. 이 구조는 SubByte, ShfteRow 그리고 Mixcolumn의 연산블록이 각각 1개씩 존재하게 된다. AES 암호의 총 10라운드를 1클록에 처리하기 위한 파이프라인 구조를 그림 10과 같이 설계하였다. 이 구조에서 SubByte, ShfteRow 그리고 Mixcolumn은 매 라운드마다 설치되었다.

표 2는 본 논문에서 제안한 두 테스트 AES 프로세서들의 성능 및 하드웨어 크기를 비교한 표이다. 비-파이프라인 구조의 AES 프로세서는 HDL로 기술하였으며 Xilinx FPGA XCV3200E를 타겟으로 합성하였다. 그 결과 동작주파수 33MHz에서 422Mbit/s로 성능을 보였다. 파이프라인 구조의 AES 프로세서는 비-파이프라인 구조와 비교하여 4.2Gbit/s의 성능을 나타내었고 회로의 크기는 3.5배 크게 측정되었다.

실제 네트워크 컴퓨터 상에서 증명하기 위하여 비-파이프라인 구조와 파이프라인 구조의 AES 프로세서를 각각 테스트 시스템에 적용하였다. 테스트 시스템으로 그림 11과 같이 TCP/IP 기반 네트워

표 2. 성능비교

구조	Clk (MHz)	Throughput (Mbit/s)	Equivalent gate counts	1 operation
Non-pipelined	33	422	91,777	10clk
Pipelined		4,224	321,184	1clk

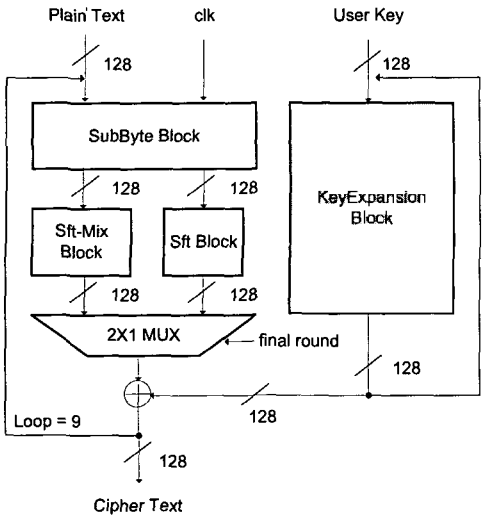


그림 9. 비-파이프라인 구조

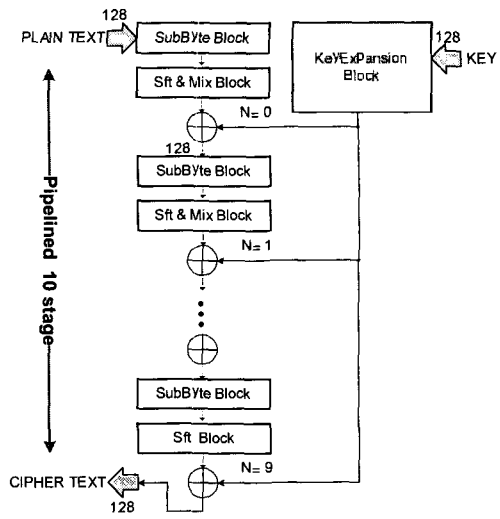


그림 10. 파이프라인 구조

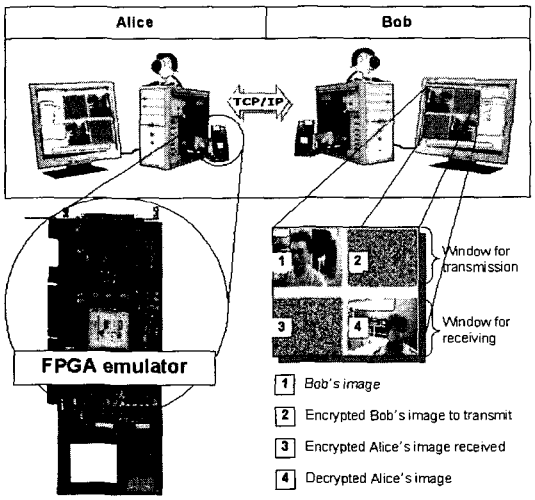


그림 11. 데모(demonstration) 시스템

크 환경에서의 동영상 데이터 암호화 전송을 이용하였다. FPGA 에뮬리이터를 이용하여 비-파이프라인과 파이프라인 구조를 각각 동영상 암호화 통신에 적용하였다. FPGA 에뮬레이터는 PCI기반 인터페이스로 네트워크 컴퓨터에 장착되었다.

성능분석 결과를 표 3에서 나타내었다. 테스트 시스템에 적용시킨 결과 비-파이프라인 AES 프로세서의 성능은 1024byte 크기의 패킷에서 15.36Mbit/s를 나타내었다. 파이프라인 구조의 AES 프로세서의 성능역시 3.5%가 증가한 15.89Mbit/s를 보였다. TPG(throughput per gate)의 경우 비-파이프라인 구조에서 3.4배 높게 평가되었다.

표 3. 성능분석 결과

구조	Clk (MHz)	Throughput(Mbit/s)		Differences(%)	
		FPGA	*Test system	H/W size	TPG (kbit/s)
Non-pipelined	33	422	15.36	91,777	0.17
Pipelined		4,224	15.89	321,184	0.05

* Input data : VGA 640×480×24bit×30frames(221Mbit/s)
* Packet size: 1024byte

3.2 모델을 이용한 AES 암호프로세서의 성능분석

모델의 검증을 위하여 BCM5820을 제안된 모델을 이용하여 시뮬레이션 한 뒤, 실제측정 결과와 비교하였다. 시뮬레이션은 Anylogic 4.5툴을 이용하였다. Anylogic은 기존의 COVERS의 후속 버전으로 중간 사양의 워크스테이션(PIV 1.7GHz, 512 MB RAM)에서 50,000개의 서로 다른 객체를 동시에 프로세싱 할 수 있는 테스트 환경을 지원한다.[9,10] Anylogic은 JAVA 언어를 기반으로 한다. JAVA는 복잡한 문제의 Data 구조와 알고리즘을 정의하기 쉽다는 장점이 있다. 또한 비주얼 모델링 언어로 사용되기 적합하며 높은 수준의 프로그래밍을 제공한다. 일반적으로 UML은 일반적 목적의 모델링 언어로서 시스템의 가공물을 정의, 시각화, 개발, 문서화하는데 사용된다. Anylogic은 UML-RT

(UML for Real Time) 모델링 기반으로 UML 모델링 기반보다 높은 구조분해 및 재사용성을 갖는다.

시뮬레이션은 패킷크기별로 나누어 수행하였다. 일정한 크기로 분해된 패킷들은 Poisson 분포로 제안된 모델의 큐 입력으로 입력된다. 포아송 분포는 시뮬레이션 툴에서 제공하는 "DistrPoisson. sample(λ)"를 이용하였으며 이때 사용된 파라미터 λ의 값은 0.4로 설정하였다. 패킷분해(packet fragment)는 라이브러리로 제공되는 "SELECTOR" 오브젝트와 JAVA언어로 기술하였고, 네트워크 컴퓨터의 입력인 NIC 부분은 "FIFO QUEUE" 오브젝트를 배치하였다. 디코딩지연과 암호프로세서의 처리시간은 "DELAY" 오브젝트를 이용하였다.

모델로 입력된 패킷은 큐 내의 대기시간, 디코딩지연 그리고 프로세서의 처리시간을 거쳐 출력된다. 디코딩지연과 프로세서의 처리시간은 테스트 프로그램(그림 6)과 설계된 AES 프로세서의 처리율(표 3)을 통해 확인할 수 있다. 하지만 큐 내의 대기시간은 네트워크 입력(포아송 분포)에 따라 패킷이 큐 내에서 대기하는 시간이 달라질 수 있다. 성능은 패킷이 모델의 큐로 진입하여 출력되기까지의 총 시간(Latency)을 측정하여 식 3.1과 같이 계산하였다. 시뮬레이션은 동일한 패킷크기만을 이용하였으며 통계적 신뢰성을 위하여 100회 반복하였다.

$$Throughput(Mbit/s) = \frac{TOTAL\_FILE\_SIZE}{Latency_{packet\_length}}$$

(식 3.1)

(packet_length = 64, 128, ···, 32768, 65,536byte)

시뮬레이션 모델은 그림 12와 같다. 파이프라인 AES와 비-파이프라인 AES를 각각 성능분석 할 수 있도록 모델링 하였다. 입력 트래픽은 100Mbyte 파일을 각각 64/128/···/8kbyte의 패킷으로 분해하여 입력시켰다. 전체응답시간(latency)은 100Mbyte의 파일이 최초 모델의 큐에 입력되는 시점부터 AES 프로세서를 거쳐 모두 처리된 시점까지로 정의하였다. 이때의 성능(throughput)은 식 3.2와 같다.

Throughput=100Mbyte/Latency (Mbit/s)

(식 3.2)

파이프라인 구조의 AES 프로세서의 성능은 33 MHz의 동작속도를 기준으로 정하였다. 이때의 처리능력은 33MHz×128bit=4.2Gbit/s이다. 예를 들어 4.2Gbit/s의 AES 프로세서는 1kbyte 패킷 하나를 처리하는 데에 약 2×10-6초의 시간이 걸린다. 비-파이프라인 구조의 경우 1kbyte 패킷을 처리하는 데이는 약 2×10-5초가 걸린다. 이 시간들을 각각 파이프라인과 비-파이프라인 AES 프로세서의 성능에 관한 파라미터로 입력하였다. 패킷 크기를 변화시키며 시뮬레이션 한 뒤 그림 13과 같은 결과를 확인하였다. 두 AES 프로세서의 성능은 패킷의 크기가 8192byte까지 평균 6.5%만을 나타내었다. 특히 1024byte의 패킷을 입력했을 때, 파이프라인 구조의 AES 프로세서는 16.37Mbit/s를 비-파이프라인 구조는 15.75Mbit/s로 4.0%의 성능향상만을 확인하였다.

Ⅳ. 결 론

본 논문은 AES 암호프로세서의 성능분석모델을

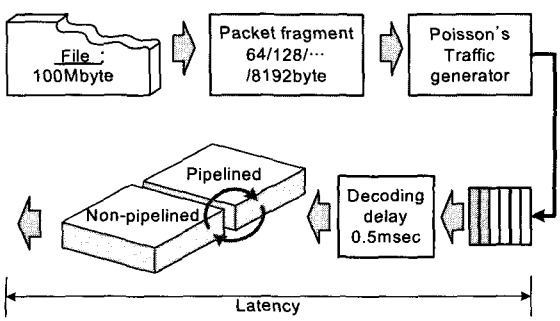


그림 12. AES 암호프로세서 성능분석모델

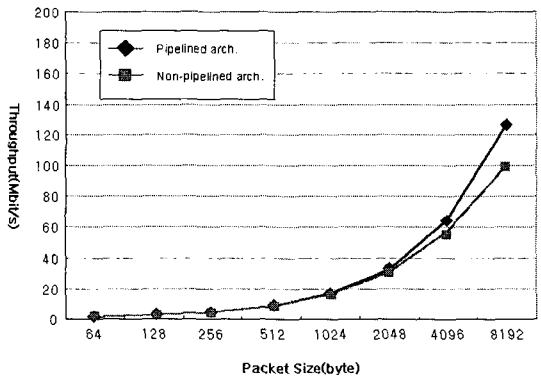


그림 13. AES 암호프로세서의 시뮬레이션 결과

제안하였다. 제안된 모델은 M/M/1 큐잉 모델을 기반으로 포아송 분포를 트래픽 입력으로 가정하였다. 모델을 이용한 성능분석결과 1kbyte 패킷 크기에서는 AES 파이프라인 구조가 비-파이프라인 구조에 비하여 4.0% 정도의 성능향상만을 기록하였다. 본 논문에서는 네트워크 컴퓨터에 장착된 암호프로세서의 성능저하 원인은 패킷이 입력된 뒤 암호프로세서까지 전달되는 경로에서 발생되는 지연 때문임을 밝혔다. 이 때 발생되는 지연시간을 제안된 모델에 적용하기 위한 파라미터로 디코딩지연이라고 정의하였다. 시뮬레이션을 통해 동일 데이터 량을 전송할 경우, 패킷크기가 작을수록 디코딩 횟수가 증가하며 암호프로세서의 성능이 낮아짐을 확인하였다.

암호프로세서가 장착된 네트워크 컴퓨터의 성능을 향상시키기 위해서는 패킷의 크기를 증가시키는 방안과 디코딩지연을 감소시키는 방안이 있다. Gbit/s 처리능력을 갖는 AES 프로세서가 최대성능을 내기 위해서는 패킷크기가 100kbyte 이상이 되어야 한다. 현재 네트워크 구성요소들의 발전 속도를 감안할 때, 패킷크기의 증가를 위해서는 상당한 시일이 필요하다. 디코딩지연의 감소는 네트워크 프로토콜을 하드웨어로 처리함으로서 가능하다. 현재 국내의 Wiznet, 미국 펜실베니아 대학의 Protocol Booster[14] 등의 연구가 그 대표적인 예이다.

PCI FPGA 애뮬레이터에서 AES 암호프로세서를 구현한 결과 파이프라인 구조는 비-파이프라인 구조와 비교하여 하드웨어 면적은 3.5배 크게 측정되었으나 성능은 3.5%의 미비한 증가만을 나타내었다. 이 결과는 모델을 통해 분석된 4%의 성능향상과 비교할 때, 0.5%의 차이이다. 즉, 네트워크 컴퓨터에서의 암호프로세서의 성능이 제안된 모델을 통해 정확하게 분석되었음을 확인할 수 있다. 본 성능분석 모델은 단일 칩 암호프로세서 설계 시, 파이프라인 구조의 AES 프로세서가 갖는 하드웨어를 축소하고, 병목의 원인이 되고 있는 공개키 프로세서의 설계면적을 확보하기 위한 기준으로 활용될 수 있다.

참 고 문 헌

[1] M. Merkow and J. Breithaupt, The Complete Guide to Internet Security, AMACOM, 2000

[2] M. McLoone and J.V. McCanny, "A single-chip IPSec cryptographic processor," IEEE Workshop on Signal Processing Systems. pp. 133-138, Oct. 2002

[3] Broadcom Co., BCM5820 Product Brief, http://www.broadcom.com

[4] CAVIUM co., IPSec/SSL NITROX-XL NHB Acceleration Boards Product Brief, http://www.cavium.com

[5] C. Fraleigh and S. Moon, "Packet-level traffic measurements from the SPRINT IP backbone," IEEE Journal of Network, vol. 17, pp. 6-16, Nov. 2003.

[6] Ho Won Kim and Sunggu Lee, "Design and implementation of a private and public key cryptoprocessor and its application to a security system," Consumer Electronics, IEEE Transactions on, vol. 50, Issue 1, pp. 214-224, Feb 2004.

[7] S. Miltchev and S. Ioannidis, "A study of the relative costs of network security protocols," In Proceedings of USENIX Annual Technical Conf., Freenix Track, pp. 41-48, June 2002.

[8] I. Cao and M. Anderson, "Web server performance modeling using an M/G/1/K* PS queue," 10th Int'l. Conf. on Telecommunications, vol. 2, pp. 1501-1506, Feb. 2003.

[9] A.V. Borshchev and Y.G. Karpov, "System modeling, simulation and analysis using COVERS active objects," IEEE Workshop on Engineering of Computer Based Systems (ECBS '97), pp. 220-227, Mar 1997.

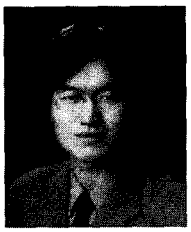
[10] XJ Technologies, Anylogic4.5 Product Overview, http://www.xjtek.com.

[11] 최병윤, 박영수, "모듈화된 라운드 키 생성회로를 갖는 AES 암호 프로세서의 설계," 정보보호학회 논문지, 제 12권, 5호, 15-25쪽, 2002년 10월.

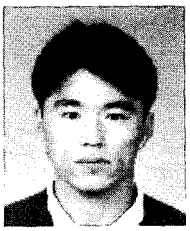
[12] National Institute of Standards and

Technology, Announcing the Advanced Encryption Standard (AES), http://csrc.nist.gov.
[13] 안하기, 신경욱, "AES Rijndael 블록 암호 알고리듬의 효율적인 하드웨어 구현," 정보보호학회 논문지, 제 12권, 2호, 53-63쪽, 2002년 4월.
[14] D.C. Feldmeier and T.M. Raleigh, "Protocol boosters," IEEE Journal on Selected Areas in Communications, vol. 16, Issue 3, pp. 437-444, April 1998.

〈著者紹介〉

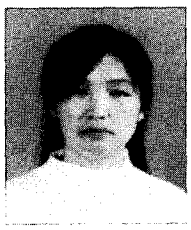


윤 연 상 (Yeonsang Yun) 학생회원
2004년 2월: 충북대학교 전기전자공학부 학사
2004년 3월~현재: 충북대학교 정보통신공학과 석사과정
〈관심분야〉 디지털 회로설계 및 테스트, 임베디드 시스템, 암호 시스템



조 광 두 (Kwangdoo Jo) 정회원
1995년 2월: 서울시립대학교 전자공학과 학사
1999년 3월~현재: 충북대학교 정보통신공학과 석사과정
〈관심분야〉 회로의 배선 모델링 및 설계, RF소자 모델링

김 용 대 (Yongdae Kim) 정회원
1990년 2월: 충북대학교 정보통신공학과 학사
1993년 2월: 충북대학교 컴퓨터공학과 석사
1989~1998년: 신흥기술연구소 팀장
2000~현재: 충북대학교 정보통신공학과 박사과정
〈관심분야〉 Computer arithmetic, ASIC 설계, 암호 시스템



한 선 경 (Seonkyoung Han) 정회원
1991년 2월: 충북대학교 정보통신공학과 학사
1993년 2월: 충북대학교 정보통신공학과 석사
2004년 8월: 충북대학교 정보통신공학과 박사
2005~현재: 특허청 전기전자심사국 심사관
〈관심분야〉 Computer arithmetic, Cryptographic system, ASIC 설계

유 영 갑 (Younggap You) 정회원
1975년: 서강대학교 전자공학과 학사
1975~1979년: 국방과학연구소 연구원
1981년: Univ.of Michigan, Ann Arbor 전기전산학과 석사
1986년: Univ.of Michigan, Ann Arbor 전기전산학과 박사
1986~1988년: 금성반도체 (주) 책임 연구원
1993~1994년: 아리조나 대학교 객원교수
1998~2000년: 오레곤 주립대학교 교환교수
1988~현재: 충북대학교 정보통신공학과 교수
〈관심분야〉 VLSI 설계 및 테스트, 고속 인쇄회로 설계, 암호학