情 報 保 護 學 會 誌
第 12 券 第 3 號, 2002. 6

고속 암호연산 프로세서 개발현황

주 학 수*, 주 홍 돈*, 김 승 주*

요 약

전자상거래의 트래픽이 엄청나게 증가하고 많은 사용자들이 안전한 온라인 거래를 요구함에 따라 고속 암호연산 프로세서의 필요성은 증대되고 있다. 고속 암호연산 프로세서란 복잡한 연산이 많은 암호방식의 연산 속도를 가속시키기 위한 보조프로세서이다. 본 고에서는 암호 사업분야 중 고속 암호연산 프로세서의 필요성을 알아보고 국내·외 제품들을 분류한 뒤 프로세서들의 기능, 성능비교 및 안전성을 위주로 조사·분석하였다. 또한 고속 암호연산 프로세서의 전망 및 발전방향을 알아보고 프로세서가 사용되는 SSL가속기, IPSec가속기, HSM, 스마트카드 제품들의 성능을 위주로 소개하기로 한다.

1. 서 론

수년동안 데이터를 암호화하는 기술은 암호에 사용되는 많은 수학연산을 처리하기 위해 높은 컴퓨팅 파워를 요구한다는 이유로 인해 웹사이트에서의 신용카드 구매와 같은 경우를 제외하고는 대부분의 비지니스에서 사용되지 않았다. 그러나, 최근에는 자신들이 가지고 있는 서버에 간단하게 add-on 보드 혹은 appliance 고속암호연산 프로세서 제품들을 장착하여 암호화의 수행을 빠르게 연산 가능하도록 할 수 있게 되었다.

회사의 경영자들은 업무가 네트웍 의존적이 되어감에 따라 더 나은 보안을 요구할 것이며 동시에 많은 소비자들은 보안 허점이 많은 인터넷을 안전하게 만들도록 요구하고 있다. 이에 따라 IDC는 2005년에는 모든 인터넷 트래픽이 암호화되는 수준으로 발전할 것이라 예측하고 있다. 물론, 하드웨어의 미래는 아직도 불투명하지만, PC에 암호연산 프로세서가 기본적으로 탑재되는 날도 멀지 않을 것으로 예측하고 있다[20].

범용 프로세서가 전자상거래에 필요한 암호화를 효율적으로 다룰 수 있도록 지원하지 못하는 반면, 고속 암호연산 프로세서는 암호연산을 빠르게 수행하도록 특별하게 디자인되어 전자상거래 서버들이 암호연산 프로세서를 이용하지 않을 때보다 90% 가량 늘어난 처리를 할 수 있게 한다. 또한 암호 연산 프로세서는 서버의 성능을 향상시키고 처리 지연을 줄일 뿐만 아니라, 새로운 하드웨어 투자를 늘릴 수 있으면서 서버의 안전성에 도움을 준다. 즉 항상 많은 작업을 하는 서버는 불안정하기 때문에, 서버에 큰 부하가 되는 암호 기능을 분리하여 프로세서가 처리함으로서 전체 시스템의 수명을 개선해 주는 경제적 이점이 있다. 또한 암호연산 프로세서는 OS나 응용프로그램 대신에 전용하드웨어가 알고리즘의 정확한 구현을 보장할 뿐만 아니라, 암호 키와 중요한 데이터를 물리적으로 보호함으로써 높은 안전성을 보장한다. 이러한 고속 암호연산 프로세서의 필요성을 정리하면 표 1과 같다.

〔표 1〕 고속 암호연산 프로세서의 필요성

내용	설명
시스템의 성능 향상	90% 이상의 성능 향상
비용 대비 효과 증가	새로운 서버 설치 비용 감소
하드웨어 투자의 주기가 늘어남	과도한 부하의 경감으로 시스템 수명 증가
서버의 안정성(Stability) 향상	부하의 감소로 인한 안전성 향상
보안성 향상	암호 키와 중요한 데이터를 물리적으로 보호

그러나, 고속 암호연산 프로세서가 모든 부분에

* 한국정보보호진흥원(KISA) ({hsju,hdjoo,skim}@kisa.or.kr)

적용되는 것이 아니라 여러 가지 분야와 목적에 따라서 그에 맞는 제품들이 존재한다. 이러한 제품들을 보안 하드웨어[1]라고 한다. 표 2는 암호연산 프로세서가 탑재된 보안 하드웨어와 관계된 제품들을 용도에 따라 분류하여 각 분야별로 주요 회사들을 정리한 것이다.

〔표 2〕 보안 하드웨어의 분류

분야	내용	주요 회사
고속 암호연산 프로세서	다양한 암호 알고리즘을 집적	Hi/Fn, Andes Network, Corrent, Broadcom, Securelink 등
SSL /IPSec 가속기	SSL(IPSec)등의 속도와 보안 비도를 높이기 위해서 사용	Rainbow Technologies, nCipher, Chrysalis-ITS 등
HSM	키관리 등의 다양한 기능을 내장	Rainbow Technologies, nCipher ,Chrysalis-ITS 등
기타	암호서버, 하드웨어토큰 등	Cylink, Rainbow Technologies 등

※ HSM : Hardware Security Modules

본 고에서는 분류된 보안 하드웨어 제품들 중에서 기반이 되는 고속 암호연산 프로세서들의 성능비교 및 기능비교, 안전성을 중심으로 소개한다. 그리고 나서 이에 대응하는 국내의 현황을 알아본다. 또한 암호연산 프로세서의 응용시장으로 큰 시장을 형성하고 있던지 또는 향후 큰 시장을 형성할 것으로 예측되고 있는 SSL/IPSec가속기, HSM 등과 같은 제품들의 개발현황을 소개하기로 한다.

II. 고속 암호연산 프로세서

본 절에서는 앞에서 분류한 보안 하드웨어 제품군 중에서 암호프로세서의 성능 비교, 안전성 및 기능에 대하여 조사·분석하였다. 고속 암호연산 프로세서는 서론에서 언급한 바와 같이 다양한 암호 알고리즘을 집적하여 구현한 것으로 많은 블록 암호 알고리즘과 공개키 알고리즘을 구현하고 있다. RC4, DES와 같은 블록 암호알고리즘의 경우에는 프로세서에 적은 부하를 주므로 보안 하드웨어와 통신을 하는데 필요한 시간 지연과 추가되는 작업을 고려한다면, 연산 성능의 측면에서는 영향이 별로 없다. 그럼에도 블록암호알고리즘을 하드웨어로 구현하는 것은 FIPS 140-1[2]의 보안 레벨을 높일 수 있고 값싸고 효율적인 하드웨어를 사용하여 AES 등과 같이 RC4보다는 느린 블록 암호알고리즘 등의 속도를 높이기 위해서 사용된다. 그러므로 본 고에서는 암호 프로세서의 성능을 단순 비교하는 경우에는 공개키 처리 속도로 비교를 하였다.

1. 성능 비교

암호연산 프로세서에서 가장 중요한 것은 속도이다. 특히, 대칭키보다는 프로세서에 많은 영향을 미치는 공개키 암호의 속도가 중요하다. 다음의 표 3에서는 시장에서 영향력이 있는 제품들에 대하여 정리를 하였다. 먼저, Hifn 제품은 저속 프로세서에서 시장 점유율이 높으므로, 다른 프로세서들에 비하여 조금은 성능이 떨어지지만 가격경쟁력과 브랜드 이미지가 있어서 아직까지는 시장에서 우위를 차지하고 있다. 다음으로 Corrent와 Andes의 암호연산 프로세서는 특히 고속 암호연산 프로세서 부분에서 높은 시장 점유율을 가지고 있는 Broadcom을 목표로 암호연산 프로세서 시장을 노리고 있는 제품들이다. 그리고 Motorola와 Intel은 통신용 프로세서 및 범용 프로세서 시장에서 시장 지배력을 가지고 있는 회사들로서 범용 프로세서에서 암호연산 속도를 높이는데 주력하고 있다. 다음에서 제시된 제품에 대한 성능은 각 사가 공개한 data sheet를 기준으로 작성하였다.

〔표 3〕 암호연산 프로세서의 성능 비교 (초당 연산회수)

	Hifn (Hi/Fn 8065)	Corrent (CR 7020)	Broadcom (BCM 5821)	Andes (Zoo)	Motorola (MPC 190)	Intel (Itanium)
RSA (1024 bit)	2,000	5,000	4,000	15,000	500	1,000

2. 안전성 비교

안전성의 측면에서는 암호 프로세서를 판단하는 가장 간단한 방법은 NIST의 FIPS 140-1을 만족하는지 여부이다. FIPS 140-1은 Level 1~4[3]까

1) 보안하드웨어란 보안 프로토콜(IPSec, SSl/TLS 등)의 성능 한계를 극복하고 또한 안전한 키관리 및 저장을 위한 하드웨어 기반의 보안장비들을 일컫음.

2) 1995년 7월 미국 NIST와 캐나다 주정부의 CSE가 공동으로 개발한 암호 모듈 검증을 위한 프로그램

지로 나누어져 있다. 다음의 표 4에서는 위에서 살펴본 제품에 대하여 인증여부와 인증 받은 level에 대하여 정리를 하였다. 이는 제품의 data sheet를 정리한 것으로 아직 인증을 받지 않은 제품도 뒤에 인증을 받을 것으로 예측되기 때문에 시장에 주는 영향은 없을 것으로 판단되지만, 국내에서 생산한 제품들의 경우에는 이러한 FIPS 인증을 받는 것이 쉽지 않을 것이므로, 어려움이 있을 것으로 판단된다.

〔표 4〕 FIPS140-1 인증 여부

	Hifn (Hi/Fn8065)	Corrent (CR 7020)	Broadcom (BCM5821)	Andes (Zoo)	Motorola (MPC190)	Intel (Itanium)
FIPS 140-1 Level	3	3	3	-	-	-

3. 기능 비교

위에서 암호연산 프로세서들의 속도와 안전성에 대하여 비교하였다. 다음은 암호연산 프로세서들을 비교할 수 있는 항목인 암호연산 프로세서들이 지원하는 알고리즘의 종류에 대하여 각 제품들의 data sheet를 참조하여 정리를 한 것이다.

〔표 5〕 암호 알고리즘 지원

	Hifn (Hi/Fn8065)	Corrent (CR 7020)	Broadcom (BCM5821)	Andes (Zoo)	Motorola (MPC190)	Intel (Itanium)
RSA	Y	Y	Y	Y	Y	Y
ECC	N	N	N	N	Y	N
RC4	Y	Y	Y	Y	Y	N
MD5	Y	Y	Y	Y	Y	N
SHA1	Y	Y	Y	Y	Y	N
AES	Y	Y	Y	N	N	N
3DES	Y	Y	Y	N	Y	N
RNG	Y	Y	Y	N	Y	N

3) · Level 1 : 가장 기본 등급의 안전성을 보장
· Level 2 : Level 1에 물리적 보안 매커니즘 부분을 보완시킨 등급
· Level 3 : Level 2에 tamper-evident가 포함된 물리적 보안 매커니즘을 보완시킨 등급
· Level 4 : 표준안에서 제정한 가장 높은 안전성을 제공하는 등급

위의 표 5에서와 같이 ECC를 지원하는 암호 프로세서조차 거의 없는 것처럼 대부분의 암호연산 프로세서들은 최근에 새로 제안된 암호 알고리즘에 대한 지원을 하지 않고, 기존에 많이 사용하고 있는 알고리즘에 대한 지원만을 하고 있으므로, 이는 암호연산 프로세서 시장에서 새로운 알고리즘을 지원하는 것은 크게 문제가 되지 않고, 공통으로 많이 사용하는 암호 알고리즘에 대한 지원만은 필수적이라고 생각할 수 있다.

4. 시장전망

암호연산 프로세서 분야는 IPSec 부분을 중심으로 발전했지만, 전자상거래가 활성화됨에 따라서 구현이 쉬운 SSL이 새롭게 주목을 받고 있다. Gartner사의 보고서에 따르면 IPSec에 비하여 SSL 프로세서 시장의 연평균 증가율은 월등히 높으며 2005년에는 전체 시장 규모가 약 4억 달러에 이를 것이라고 전망했다[13].

〔표 6〕 암호 프로세서 시장 전망 (단위 백만 달러)〔13〕

	1999	2000	2001	2002	2003	2004	2005	CAGR (%) 2000 - 2005
Total	54.1	86.3	97.6	141.7	206.0	286.2	394.2	36
SSL	0.9	5.4	19.8	38.4	66.3	104.4	166.9	99
IPSec	53.2	80.9	77.8	103.3	139.7	181.8	227.3	23

5. 국내현황

국내 암호연산 프로세서 제품들은 표 7에서 알수 있듯이 공개키 암호 프로세서 보다 대칭키 암호 프로세서 제품 위주라는 것을 알 수 있다. 또한 국내 제품의 경우에는 속도에 대한 자료가 거의 없고, 있다 하더라도 1초에 100회 정도의 RSA 1024bit의 연산을 하는 것으로 알 수 있다. 앞 절에서 제시된 국외의 프로세서와는 비교의 대상이 거의 되지 않지만 최저 약 4배에서 최고 약 100배 정도의 차이가 나는 것을 알 수 있었다. 또한 국외의 HiFn과 같은 회사에서도 2-3년 전에는 주로 판매되는 제품들이 200회 정도의 속도를 가지고 있었지만, 현재는 이보다 빠른 제품을 출시하고 있음에 반하여 국내 제품의 경우에는 성능에 대한 향상이 거의 없는 것으로

보인다. 이는 국내 암호 프로세서에 대한 시장이 거의 형성이 되지 않아 제품에 대한 수요가 없음에 기인한다고 판단된다. 표 7은 국내 암호프로세서 제조업체들을 분류하고 분류된 제품들에 대한 암호기능 및 속도를 정리한 것이다. 표는 홈페이지에 제시된 data sheet에 따라 작성된 것이며 표에서 "×" 는 지원되지 않음을 뜻하며 "-" 는 해당되는 자료가 없었음을 의미한다.

〔표 7〕 국내 암호연산프로세서 제품 기능 및 성능

	회사명/제품명	암호함수		성능	
		대칭키	공개키	대칭키	공개키
국내 암호연산 프로세서	시큐어 파아 (Crypto Engine)	SEED DES 3DES AES	×	SEED (246Mb) DES (356Mb) 3DES (107Mb) AES (256Mb)	×
	시큐 아이티 (지문인식 스마트 카드)	×	×	×	×
	아라리온 (Cipher)	DES, SEED, 3DES	×	DES (50Mb)	×
	퓨처 시스템 (Secuway Gate 2000)	SEED, DES, 3DES, RC5, CAST (128), Blow-fish, Crypton	×	-	×
	텔레 시큐어 (CNISTTM)	128bit Enc Alg	×	5 Mb with 5V	×
	시큐리티 테크놀로지스 (암호 프로세서 SCC 101,102)	×	RSA	×	RSA (124Kbits/s)
	시큐리티 테크 놀로지스 (암호보드 SCC CryptoXL)	DES, SEED 3DES, RC4 해쉬 (SHA1,MD5)	×	SEED (200Mb) DES (245Mb) 3DES (80Mb)	×

Ⅲ. SSL 가속기

본 절에서는 암호연산 프로세서를 이용한 보안하드웨어 제품들 중 SSL 가속기, IPSec 가속기, HSM, 스마트 카드 등 제품들의 성능을 위주로 조사하였다. 보안 프로토콜에 의존하는 시스템 중 대표적인 예로 SSL 가속기와 IPSec 가속기가 있는데, 먼저 SSL 가속기에 대하여 살펴보도록 한다. 암호 가속기 시장은 nCipher, Rainbow, Broadcom과 Ingrian 등의 회사에서 장악하고 있어, 위의 회사들의 암호 제품의 성능 및 안전성에 대하여 비교 정리한다.

SSL이란 일반적으로 Web의 보안을 위해서 사용되는 프로토콜이다. SSL을 이용하여 Web에 보안 기능을 추가하면 Web Server의 성능이 떨어지게 된다. 보안 기능을 가속기에서 처리하도록 하는 경우에는 중앙처리장치에서는 여유시간이 많아져서 좀 더 많은 사용자들에게 Web 서비스를 할 수 있다. 즉, 서명생성과 검증을 비롯해 비밀키의 키 교환에 필요한 수학적 연산 과정은 많은 계산 능력을 필요로 한다. SSL은 CPU의 90%이상을 점유해야 하기 때문에 수백, 수천 개의 클라이언트와 동시에 SSL session을 유지해야 하는 웹 서버는 과부하(overload)로 인해 긴 응답시간(response time)을 유발하는 것을 막을 수 있다. 그러나, SSL은 패킷을 암호화하기 때문에 URLs, cookies, application headers 등을 관찰해서 그 결과에 따라 라우팅을 결정하는 트래픽 관리 어플리케이션들의 기능을 발휘하지 못하게 한다. 표 8은 SSL 가속기 시장에서 시장 점유율이 높은 제품들과 몇 가지 성능이 좋은 제품들에 대한 성능의 비교표이다. 다음의 표는 제품들의 data sheet에 따라 작성한 것이며 SSL가속기의 성능을 알 수 있는 초당 가속기가 다룰 수 있는 새로운 SSL 트랜젝션(transaction)의 수를 나타내는 TPS(Transaction Per Second)를 조사 정리한다.

시장에서 가장 많이 사용되는 제품인 Rainbow, nCipher등의 제품에서는 제공하는 TPS가 그렇게 높지 않은 것은 아직까지는 SSL 가속기의 시장이 성능 위주로 크게 발전하지 않았다는 것을 알 수 있으며, Andes Network과 같이 새로 시장에 진입하는 제품들의 경우에는 주로 성능을 위주로 시장에 진입을 노리고 있음을 알 수 있다.

특히, Andes Netwok에서 나온 제품은 위에서 설명한 일반적인 SSL 가속기 제품들과는 달리 시스

템으로 들어온 Packet들을 Record 단위로 모아서 처리하는 것이 아니라, Packet 단위로 처리하는 새로운 방식을 사용하여 SSL 메시지를 처리하는 속도를 높였다[19].

〔표 8〕 SSL 가속기의 성능 비교

회사	Server Termination 방식		Appliance Termination 방식			Co-Appliance Termination 방식
	nCipher (nForce 400 SCSI)	IVEA Tech (CryptoSwift 600)	Rainbow (NetSwift 2012)	Ingrian (i140)	Intel (Net Structure 7115)	Andes (PSSL 6000)
TPS :Transaction Per Second	400	600	1000	300	1200	5000

Gartner사의 보고서[13]에서는 SSL가속기 시장을 크게 웹 서버 시장(server termination[4] 방식)의 제품과 로드 발란싱 스위치 시장(appliance termination[5] 과 co-appliance termination[6] 방식의 제품)으로 구분하여 전망하고 있는데, 웹 서버 시장 중심에서 점차 스위치 시장 중심으로 옮겨 갈 것으로 예측하고 있다.

〔표 9〕 SSL 가속기의 시장 전망〔13〕 단위 : 백만 달러, NM =Not Meaningful

	'99	'00	'01	'02	'03	'04	'05	CAGR (%) 2000-2005
Total Market	0.9	5.4	19.8	38.4	66.3	104.4	166.9	99
Web Server	0.9	5.4	15.3	25.0	36.1	49.6	67.5	66
Load-balancing Switch	0.0	0.0	4.6	13.4	30.2	54.8	99.4	NM

4) PCI나 SCSI방식으로 서버에 직접적으로 연결되며 카드 형태로 서버 내부에 삽입되어 서버의 부하를 낮추어 줌

5) 스위치와 라우터(혹은 게이트웨이)사이에 위치하며 네트워크 선상에 직접 연결되는 stand-alone device이며 모든 네트워 트래픽을 감시해 SSL 트래픽일 경우에만 처리

6) 스위칭 장비와 같은 네트워크 관리 장비에 연결되어 SSL 기능을 수행하며 appliance termination 과 달리 모든 네트워 트래픽을 감시할 필요가 없고 스위칭 장비에 의해 분리 전송되어오는 SSL 트래픽만을 처리

Ⅳ. IPSec 가속기

IPSec은 IP 패킷의 무결성, 인증, 기밀성 등의 보안 서비스를 지원할 수 있는 보안 프로토콜의 개발을 위해서 만들어 졌다. 따라서 AH(Authentication Header)는 패킷의 무결성과 송신자 인증서비스를 위한 서비스를 제공하고 ESP(Encapsulating Security Payload)는 무결성과 인증서비스이외에 기밀성 서비스를 추가로 제공한다. 위의 2개의 AH와 ESP 모드는 독립적으로 사용할 수도 있고 같이 사용될 수도 있으며, 각각 AH와 ESP 모드는 Transport 모드와 Tunnel 모드로 나누어진다. 기본적으로 Transport 모드는 IP와 TCP header 사이에 AH와 ESP Header가 들어가는 구조이고, Tunnel 모드에서는 기존의 IP Packet의 내용 전부를 AH 또는 ESP Header 안에 넣고, 이 자료를 전송하기 위한 새로운 IP Header를 형성하는 구조로 되어 있다. IPSec의 경우 SSL과 마찬가지로 기능을 분리할 수도 있지만, 실제적으로는 VPN 제품에 탑재되는 경우가 많아서 분류를 하지 않고 단순하게 사용되는 암호 연산 프로세서를 이용하여 성능을 비교하였다. IPSec의 성능비교는 세계 VPN Chip 시장의 75%를 차지하고 있는 Hifn의 제품와 Hifn의 주요 경쟁자인 Broadcom을 비교의 대상으로 두었다. 그리고, 이들 보다는 시장점유율에서는 떨어지지만 성능면에서 월등한 몇 개의 제품을 가지고 있는 신생 기업들의 제품과 비교를 하였다. 표 10은 각 제품의 data sheet를 기본으로 하였다.

〔표 10〕 IPSec 가속기의 성능 비교(CHIP에 의한 비교)

회사	Broadcom	Corrent	HiFn	Motorola	Chrysalis-ITS
암호연산 프로세서	BCM 5840	PacketArmor 7020	HiFn II	MPC190	LUNA - VPN
IKE (1024 bit DH) connection/sec	1200 (BCM 5820)	-	1500	520	-
Encrypt Through put(Mb)	2400	2500	2048	600	100

* 3DES + SHA-1을 사용하는 경우 속도 비교를 한 자료임

VPN의 경우 Node에서 Node로 들어오는 모든 메시지가 대칭키에 의하여 암호화되어야 함으로, 비대칭키의 암/복호화의 속도 측면이외에도 대칭키의

암/복호화 속도도 무시를 못하는 요소임으로 위에서 암호화의 속도를 비교할 때 Mbps 단위로 비교를 하였다.

V. 기타(HSM, 스마트카드)

HSM(Hardware Security Module)이란 PCI, SCSI 인터페이스를 통해 서버에 연결되어 있는 하드웨어 암호 디바이스이다. HSM은 다양한 하드웨어와 소프트웨어 토큰에 의해 보호되는 매우 높은 키 관리 기법을 제공한다. 대표적인 특징은 하드웨어 기반의 암호연산(예를 들어 난수 생성, 키 생성, 전자서명, 키 저장 및 복구 등)과 같은 기능들을 제공한다. 또한 비대칭형 암호연산에 사용되는 개인 키들의 하드웨어 보안(물리적 보안), 개인 키들의 안전한 관리, 암호연산의 가속기능(이 기능은 호스트 서버의 암호연산을 수행하는 부하를 격감시켜줌)들을 제공해주고 있다. 표 11은 PKI의 활성화에 따라 암호프로세서를 연구하고 있는 회사들 중 HSM의 대표적인 회사로 nCipher와 Chrysalis-its사의 제품군들을 위주로 비교 정리하였다.

〔표 11〕 HSM에서의 암호연산 성능 및 안전성 비교

회사명 (국가)	제품명		성능(No. of 1024b Sig/sec)	안전성 (FIPS Level)
nCipher (영국)	nShield	nShield F2	150	2
		nShield F3	150	3
		nShield F2-UltraSign	400/300	2
		nShield F3-UltraSign	400	3
CHRYSALIS-ITS (캐나다)	Luna Products	Luna CA(Root Key Protection)	-	3
		Luna XP plus(Sign Engine)	500	3
		Luna 2 (Signing authentication token)	-	2
		Luna RA (HSM)	-	2

스마트 카드란 메모리, CPU, COS(카드운영체제), 보안모듈 등을 갖추어 특정한 연산을 수행할 수 있는 집적회로 칩으로 각종 정보를 보관, 처리하는데 유용한 장치이다. 스마트 카드 제품들은 고속 및 고수준의 암호기능을 제공하는 보조 프로세서(Co-processor)에 의존한다. 스마트 카드는 제한된 환경 때문에 공개키 암호알고리즘의 연산 속도가 전체 스마트 카드의 처리속도에서 큰 비중을 차지하고 있다. 따라서 여기서는 제품들의 공개키 암호알고리즘의 연산속도를 중심으로 살펴본다. 표 13은 RSA에서 조사된 자료를 참고하여 스마트 카드 시장을 주도하고 있는 Thomson(ST16CF54B,ST19CF68, ST19KF16), Siemens(SLE44CR805,SLE66CX160S),Philips(P83W854/-858,P83W8516/8532),Hit-achi(H8/3111-3112),NEC(μPD789828) 제품들의 공개키 암호 중 1024비트 RSA의 속도를 제품별로 비교한 자료이다.

〔표 12〕 스마트카드에서의 암호연산 성능 비교(1)〔21〕 (ms) $e=F_4=2^{16}+1$

RSA (1024)	H8/ 3111 -3112	H8/ 3113	ST16C F54B	ST19 CF68	ST19K F16
Sign with CRT	n/a	n/a	800	400	110
Sign without CRT	n/a	480	n/a	n/a	380
Verify ($e=F_4$)	n/a	n/a	265	150	5

※ n/a : not available

〔표 13〕 스마트카드에서의 암호연산 성능 비교(2)〔21〕 (ms)

RSA (1024)	P83W8 54/858	P83W85 16/8532	SLE44 CR805	SLE6 6CX16 05	μPD78 9828
Sign with CRT	250	160	450	230	100
Sign without CRT	800	400	n/a	880	360
Verify ($e=F_4$)	50	25	n/a	24	7

VI. 결 론

전자상거래의 트래픽이 엄청나게 증가하고 많은 사용자들이 안전한 온라인 경험을 요구함에 따라 고

속 암호연산 프로세서의 필요성은 증대되고 있다. 이에 따라 본 고에서는 국외의 고속 암호연산 프로세서 제품들을 분류하고 성능, 기능 및 안전성을 위주로 비교 정리하였다. 또한 이에 대응하는 국내의 암호연산 프로세서 현황을 소개하였으며 전자상거래의 활성화에 따라 암호 프로세서의 새로운 사업영역으로 떠오르고 있는 가속기시장 및 HSM, 스마트 카드 등의 제품들의 성능을 암호연산의 성능 위주로 비교 정리하였다. 이는 앞으로 국내 암호연산 프로세서의 시장 개척 및 향후 떠오를 가속기 시장, 스마트 카드 시장에 진입하기 위해 기술력과 시장 분석력에 대한 자료로 활용될 것으로 판단된다.

〔표 14〕 암호프로세서 제품 기능 및 성능 분류(1)

회사명 (국가)	암호 프로세서	암호함수					성능				비고
		난수 생성기	해쉬 함수	대칭키	공개키	프로토콜	3DES +SHA1	3DES	공개키 (RSA operations /second	공개키 (DSA, DH operation/ second	
Hifn (미국)	HIPP (7814/ 7854)	Y	SHA1 MD5	AES DES 3DES ARC4	RSA DH	IPSec IKE	500 Mbps (7854) 200Mbps (7814)	-	-	300 IKE quick mode connections/second(7854) 120 IKE quick mode connections/s(7814)	LZS 압축기술 (특허)
	HIPP II(8154)	Y	SHA1 MD5	AES DES 3DES ARC4	RSA DH DSA	IPSec IKE	2.408 Mbps	-	-	1500 IKE quick mode connections per second	
Corrent (미국)	Packet Armor	True 3 grade randomizer(FIPS140-2)	SHA1 MD5 HMAC	DES 3DES AES	RSA DH	IPSec	-	-	-	-	Best Security Processor 선정됨 (2002년)
	Socket Armor (CR 7020)	Y	SHA1 MD5 HMAC	DES 3DES AES ARC4	RSA	SSL IPsec	-	-	5,000	-	
Broadcom (미국)	BCM 5805	Y	MD5 SHA1 HMAC	DES 3DES	DH	IPSec IKE SSL TLS	310 Mbps	-	-	250 DH key exchange/s	
	BCM 5820	Y	MD5 SHA1 HMAC	DES 3DES ARC4	RSA DH	IPSec IKE SSL TLS	310 Mbps	-	800 RSA private key signings/s	1250 DH key exchange/s	
	BCM 5821	-	SHA1 MD5 HMAC	DES 3DES ARC4	RSA DH	SSL TLS IPSec IKE	470 Mbps	-	4000	3000 DH transactions/s	
	BCM 5840	-	MD5 SHA1 HMAC	DES 3DES	N	IPSec	2.4Gbps	-	N	N	

〔표 15〕 암호프로세서 제품 기능 및 성능 분류(2)

회사명 (국가)	암호 프로세서	암호함수					성능				비고
		난수 생성기	해쉬 함수	대칭키	공개키	프로 토콜	3DES +SHA1	3DES	공개키 (RSA operation s /second	공개키 (DSA,DH operations/ second	
Andes (미국)	ZOO	-	-	-	RSA DH	SSL	-	-	15,000	-	Packetized SSL technology (특허)
Motorola (미국)	MPC 190	Y	SHA1 MD4 MD5 HMA C	DES 3DES ARC	RSA DH ECC	IKE IPSec WTLS/ WAP SSL/ TLS	-	-	520	1000 ECC(155-bit) key exchange/s	
Intel (미국)	Itanium	Y (Intel RNG)	-	-	RSA DH	SSL IPSec	-	-	1000	-	Sun UltraSPA RC III processor 보다 10배 더 빠름

참 고 문 헌

〔1〕 "VPN 보안 기술 표준 해설서 작성",한국정보보호 진흥원 2001

〔2〕 이동훈, 임채훈, "MPLS와 MPLS 기반 VPN", (주) 퓨처시스템 암호체계센터

〔3〕 "MPC190 Product" Summary Page,

〔4〕 "An introduction to IPsec", ITL Bulletin, March 2001

〔5〕 "공개키 암호 프로세서 동향", ITFIND

〔6〕 최승복, 임채훈, "SSL 가속 기술의 분류와 제품 비교", 퓨처시스템 암호체계센터

〔7〕 "The BCM5840 Product Brief", available at http://www.broadcom.com

〔8〕 "Data Sheet BCM5820", available at http://www.broadcom.com

〔9〕 "Intelligent Packet Processing" available at http://www.hifn.com

〔10〕 "Corrent Families of Security Processors" available at http://www.corrent.com

〔11〕 Carlton R.Davis, "IPSec :SECURING VPNS", McGraw-Hill

〔12〕 "NetSwitft 2012 overview" available at http://www.rainbow.com

〔13〕 J.Donovan, "Security Processors in 2001", 2001.06, Gartner Report available at http://www4. gartner.com/

〔14〕 S.Abbott, "Cryptographic Acceleration secures eCommerce and Enhance Server Performance", 2000.09, Rainbow-Technologies. http://www.rainbow.com/library/index.html

〔15〕 Tolly Group, "Intel NetStructure 7115 e-Commerce Accelerator Server Performance Evaluation", Tolly Report, 2000.12 available at http://www.tolly.com/

〔16〕 "Smasing the SSL speed Trap", Network Computing, 2001.6.11. http://www.network computing.com/

〔17〕 Networkshop, "Scaling security in ecommerce applications", Report synopsis. http://www.networkshop.ca/documents/icspreview.pdf.

〔18〕 "Scaling security in e-commerce applications", 2001, http://www.coradiant.com/services /research/whitepapers.html

〔19〕 "Packetized SSL Accelerator User's Guide", http://www.andesnetworks. com

[20] "Information Security Magazine" January, 2001 available at http://www.infosecuritymag.com/articles/january00/cover.shtml
[21] "Performance Comparison of Public-Key Cryptosystems; Smart Card Crypto-Coprocessors for Public-Key Cryptography; Chaffing and Winnowing: Confidentiality without Encryption; DES, Triple-DES and AES; DES-II Challenges Solved", RSA CryptoBytes, 1998, Volume 4, No1.

〈著者紹介〉

주 학 수 (Hak-Soo Ju)
1997년 8월 : 고려대학교 수학과 이학사
1999년 8월 : 고려대학교 수학과 이학석사
2001년 8월 : 고려대학교 수학과 박사과정 수료
2001년 9월~현재 : 한국정보보호진흥원(KISA) 연구원

주 홍 돈 (Hong-Don Joo)
1992년 2월 : 서강대학교 전자계산학과 학사
1994년 2월 : 서강대학교 컴퓨터학과 석사
1994년 2월~1999년 5월 : 삼성전자 연구원
2001년 8월 : 서강대학교 컴퓨터학과 박사과정 수료
2001년 7월~현재 : 한국정보보호진흥원(KISA) 연구원

김 승 주 (Seung-Joo Kim)
종신회원
1994년 2월 : 성균관대학교 정보공학과 공학사
1996년 2월 : 성균관대학교 대학원 정보공학과 공학석사 (암호학 전공)
1999년 2월 : 성균관대학교 대학원 정보공학과 공학박사 (암호학 전공)
1998년 12월~현재 : 한국정보보호진흥원(KISA) 암호기술팀장
2000년 6월~현재 : 한국정보통신기술협회(TTA) 정보통신기술위원회 암호기술연구반 의장
2002년 4월~현재 : 한국정보통신기술협회 국제 표준화 전문가