퍼스널 컴퓨터용 관용 암호화 시스템의 구현†

°강 성 기*, 이 진 수**, 이 상 곤***, 문 상 재*
*경북대학교 전자공학과, **대구 MBC, ***창신전문대학

Hardware implementation of a conventional cryptosystem for personal computers

°S. K. Kang*, J. S. Lee**, S. G. Lee***, S. J. Moon*
*Kyungpook National University, **Taegu MBC,
***Changshin Junior College

(Abstract)

A realization of a conventional cryptosystem for personal computers using the DSP56001 digital signal processing chip is presented. An improved Lucifer-type algorithm is employed to encrypt, and executed in the DSP56001. The Diffie-Hellman method is employed to generate and distribute the key. The implemented board can be plugged in the I/O port of personal computers.

I. 서 론

정보화 사회에서 정보 보안의 필요성은 여러 분야에서 대두되고 있다. 정보 보호의 대상은 사적인 신상 내용으로부터, 입시업무, 기업의 신제품 설계사양, 그리고 행정적인 내용등 다양하다. 최근에 퍼스널 컴퓨가 널리 보급됨에 따라 컴퓨터내에 저장되어 있는 정보가 불법적인 접근, 수정 및 유출되는 것에 대하여 사용자들의 관심이 높아지고 있다. 정보 보호를 위하여 접근의 제한, 경비자의 활용, 이해집단의 지리적 분리등 물리적 보안 방법을 채택할 수 있지만, 보다 효과적이고 경제적인 방법은 암호화 장치

†본 논문은 1990년도 체신부, 한국전기통신공사 연구비 지원에 의한 결과임.

를 사용하는 것이다[1-3].

본 논문에서는 퍼스널 컴퓨터내에서 정보보호를 위한 암호화 장치를 개발하였다. 이 장치에서는 정보를 암호화 하기위하여 블록크기가 64 비트로 변형된 Lucifer암호화 알고리듬을 사용하였고[4], 암호 및 복호를 위한 키이관리에는 공용 키이 암호화 알고리듬을 이용하였다.

하드웨어 실현에 있어서는 Motorola DSP56001을 사용하여 고속으로 데이타를 처리할 수 있도록 하였다[5]. 이 하드웨어는 기존 퍼스널 컴퓨터의 회로를 수정하지 않고 입/출력 포트에 쉽게 장착할 수 있도록 보드로 제작되었다.

Ⅱ. 데이타의 암호화

본 논문에서 채택한 관용 암호화 알고리듬은 key의 크기와 정보문 및 암어문의 블럭 크기가 128 비트인 Lucifer를 DES나 FEAL-8과 같이 64 비트로 조정한 변형된 Lucifer 암호화 알고리듬 이다. 이 변형된 Lucifer 암호화 알고리듬에 입력되는 키이, 정보문 및 출력되는 암호문의 블럭 크기는 공히 64비트이다. 변형된 알고리듬은 Lucifer 의 원형에서 키이 바이트 사용 스케쥴과 펼쳐진 콘볼루션 레지스터를 64 비트의 키이 크기에 맞도록 변형한 후, DES 처럼 대체상자 입력 이전에 평어를 확장시키고 각 대체상자가 4개의 대체표를 갖게 함으로써 키이가 바뀌어도 높은 심볼간 상호 의존도를 유지할 수 있도록 한 것이다.

암호화 과정을 구체적으로 설명 하면 다음과 같다. 암호화 과정은 같은 형태의 과정을 8번 반복 수행하며 한 라운드에 해당하는 암호화 과정은 그림 1 과 같다.

그림 1에서 입력 정보문의 64비트는 32비트씩 상반부와 하반부로 나누어진다. 한 라운드가 수행되는 과정에서 상반부 및 보조 열쇠의 영향을 받아서 새로운 32비트의 하반부가 구성되고, 이 변형된 하반부는 최종 라운드를 제외하고는 다음 라운드로 넘어가기 전에 상반부가 되고 하반부는 직전 라운드의 상반부로 대체되어진다. 각 라운드에서는 먼저 한바이트의 정보문과 한바이트의 보조 키이가 비트별 mod-2 연산을 한 다음, 두 개의 대체상자의 입력이 되기 위해서 DES와 같이 비트 확장(expansion)을 한다. 대체를 거친 바이트는 치환 과정에서 비트 자리 바꿈이 행해진다. 암호화 과정에서 마지막 과정인 확산(diffusion)은 빠른 시간에 넓게 이루어지는 것이 바람직하다. 치환 과정을 거쳐 얻어진 바이트는 하반부의 특정한 비트와 비트별 mod-2 연산을 다시

행하게 된다.

이렇게 형성된 32 비트는 다음 라운드의 상반부에, 그리고 하반부는 직전 라운드의 상반부를 그대로 사용한다. 한 라운드 과정에서는 S_0 및 S_1 의 2개의 S-상자와 하나의 P-상자가 4번 반복 수행된다. 키이 크기가 64 비트의 경우 전체 라운드 수가 128 비트의 경우에 비해 반으로 줄어들어 입력되는 키이에 따라서는 최대 100% 의존도를 얻지 못할 경우도 있다. 따라서 이런 점을 개선하기 위해서는 DES처럼 대체상자 입력 이전에 평어를 확장(expansion)시키고 각 대체상자가 4개의 대체표를 갖게 함으로써 키이가 바뀌어도 높은 상호의존도를 일정하게 유지할 수 있다. 두 개의 대체상자 S_0 와 S_1 이전에 위 설명과 같이 키이 interruption의 위치 조정과 autoclave 방식을 도입하여 확장시킨 후 대체상자에 입력하도록 한 부분이 그림 1의 점선내에 나타나 있다.

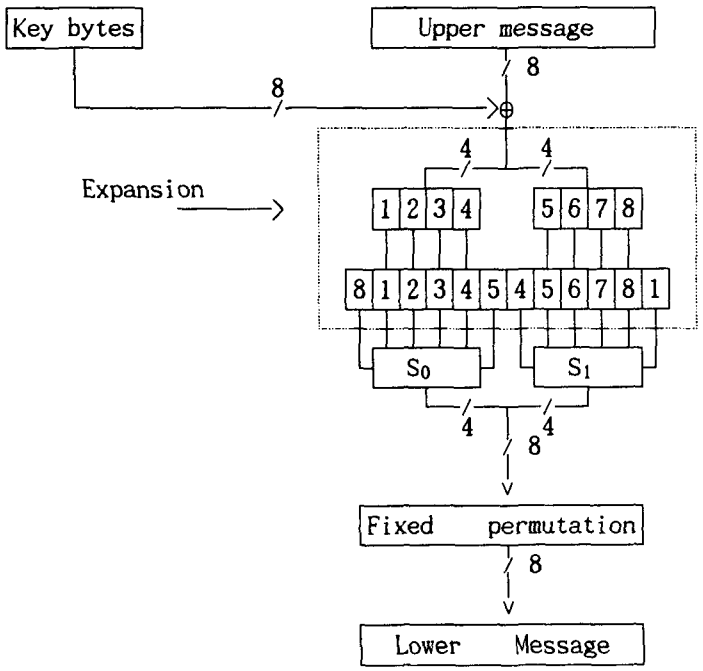

Fig. 1. The developed encryption algorithm

수신측에서의 암호해독을 위한 복호화 과정은 암호화의 역순으로 그림 1의 과정을 수행하되 키이 바이트는 키이 바이트 사용스케쥴의 아래쪽에서 위쪽으로 역순 과정으로 이루어진다.

Ⅲ. 키이 생성

정보 보호를 위한 암호화 과정에서 시스템 사용자의 인증과 필요한 세션키이(session key)를 효과적으로 관리하기 위하여는 공용 키이 알고리듬을 사용하였다. 공용 키이 암호화법에는 RSA방법[6]과 Diffie-Hellman 방법[1]등이 있으며, 본 논문에서는 하드웨어 실현에 효과적인 Diffie-Hellman 방법을 적용하였다.

Diffie-Hellman방법은 유한체에서의 멱승법으로 두 통신자간에 공통 키이를 생성할 수 있는 방법이며, 처음으로 공용키이 암호 시스템을 실현시킬 수 있는 방법을 제시한 것이다. Diffie-Hellman 방법을 간단히 살펴보면, 유한체 GF(q), q = 소수, 에서 a를 원시원이라 두면 임의의 수 x 멱승인

$y = a^X \bmod q,\ 1 < x < q - 1$

에서 y 를 계산하기는 매우 쉬우나, y 로 부터 x 를 계산 하기가 어려운 성질을 이용하여 두 통신자간에 공통 키이를 생성하는 것이다. D-H 방법에서 두 사용자간의 공통키이를 생성하는 과정은 다음과 같다. 사용자 A 가 비밀 키이 X_A 및 공개 키이 $Y_A(a^{X_A} \bmod q)$ 를 발생시키고 사용자 B 역시 같은 방법으로 비밀 키이 X_B 및 공개 키이 $Y_B(a^{X_B} \bmod q)$를 가진다. 두 통신자 A 와 B 는 각각 상대방의 공개 키이를 교환한 다음 자신의 비밀 키이를 지수승함으로써 공통의 세션 키이 $K_{AB} = a^{X_A \cdot X_B} \bmod q$ 를 생성한다.

본 시스템에서는 가입자의 공개 키이를 ROM에 저장하여 놓았으므로 통신자간의 공통의 세션 키이를 생성하여 사용할 수 있다.

Ⅳ. 암호화 시스템의 구현

본 논문에서 채택한 암호화 알고리듬 및 키이 생성을 위한 퍼스널 컴퓨터용 plug-in 회로보드를 제작하였다. 이 회로보드의 주요 구성품은 DSP56001칩, 32K×24-bit 의 EPROM, 8K×24-bit 의 RAM, 20MHz 의 발진기, 그리고 RS232C 보드 이다.

Ⅳ.1 DSP56001 의 사양및 기능

그림 2는 DSP56001 의 구조 블럭도 이며 주요 사양은 다음과 같다.

* 처리 속도 : 20.5MHz, 10.25 MIPS(million instructions per second)

1024 point complex FFT in 3.23 ms

* 데이타 ALU 구성 :
  . 2개의 48 비트 accumulator
  . 2개의 8 비트 accumulator 확장 레지스터
  . 4 개의 24비트 입력 데이타 레지스터
  . 하나의 병렬, 단일 사이클 승산기 와 논리 장치
  . 두개의 데이타 버스 쉬프터/리미터 회로
* 병렬처리 : DSP56001의 데이타 ALU, address arithmetic units, 그리고 program controller 는 병렬로 동작한다.
* Single-cycle multiply/accumulate 명령을 소유.
* 반복처리를 위한 하드웨어 DO 명령과 REPEAT(REP) 명령
* DSP56001은 6개의 on-chip 메모리, 자체내에 세가지 주변장치(SCI, SSI, and HI) 기능보유 및 클럭 제너레이터를 가진다.

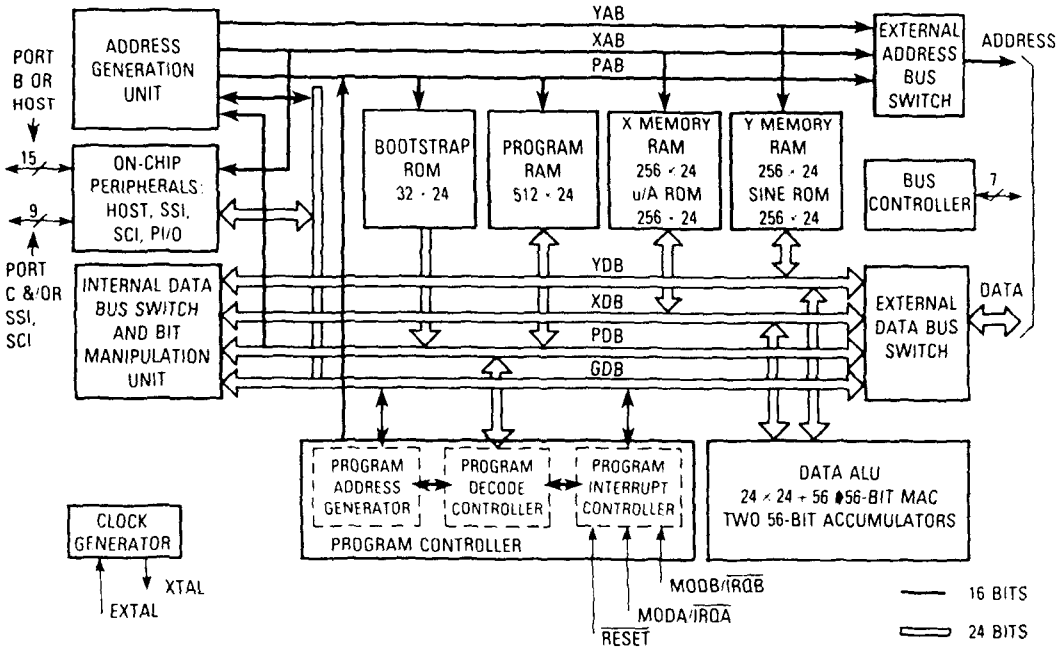

Fig. 2. DSP56001 block diagram

주요 구성 부분의 동작은 다음과 같다. DSP56001 칩내에서의 데이타 이동은 X data bus(XDB), Y data bus(YDB), Global data bus(GDB) 그리고 Program data

bus(PDB) 의 4개의 양방향 24-bit 버스로 이루어지며, 버스들간의 교환은 내부 버스 스위치에서 이루어진다.

주소 버스는 내부 X 데이타 메모리와 Y 데이타 메모리를 지정하는 단방향 16-bit X address bus(XAB)와 Y address bus(YAB), 내부 프로그램 메모리를 지정하는 양방향 24-bit Program address bus(PAB)로 이루어진다. 외부 프로그램 메모리 주소는 XAB, YAB 및 PAB를 선택하는 three-input multiplexer에 의해 지정되는 단방향 16-bit 주소 버스에 의해 지정된다.

데이타 산술논리기에서는 산술 및 논리적인 모든 연산이 수행되며, 그 구성은 4개의 24-bit 입력 레지스터, 하나의 MAC(multiply-accumulator/logic unit), 두개의 48-bit 누산기, 두개의 8-bit 누산기 확장 레지스터, 하나의 누산기 쉬프터 및 두개의 데이타 버스 쉬프터/리미터들로 이루어진다.

메모리는 프로그램 메모리와 데이타 메모리로 분류되어지며, 데이타 메모리는 X 데이타 메모리와 Y 데이타 메모리로 구분 되어진다. 또한 프로그램 메모리와 데이타 메모리를 외부에서 확장 할 수 있다. 프로그램 제어기는 프로그램 주소 발생, 명령어 디코딩, 그리고 하드웨어 DO 루프 제어 등의 처리를 수행한다.

DSP56001의 입/출력단은 다양한 시스템과의 인터페이스를 가능하게 하며, 이 입/출력단은 상당히 융통성 있는 47개 핀의 확장 포트와 24개의 부가적인 입/출력핀으로 구성된다. 이러한 핀들은 포트 B, 포트 C와 같은 일반적 목적의 입/출력단으로 사용되어질 수 있고, MPU/DMA(microcomputer unit/direct memory access), 직렬 통신 인터페이스(SCI) 및 동기 직렬 인터페이스(SSI)와 같은 주변 장치로도 사용되어질 수 있다. 특히 직렬 인터페이스는 다른 장치와의 8비트 데이타 인터페이스를 위해 전이중 방식 포트를 가지며, 인터페이스는 RXD, TXD의 3 개의 핀을 이용하고, 직접 통신 혹은 RS232C를 사용하여 통신이 가능하다. 또한 이 인터페이스의 전송속도는 사용자가 프로그램화할 수 있다.

Ⅳ.2 하드웨어 설계

그림 3은 본 연구에서 제작된 관용 암호화 시스템이며, 이 하드웨어의 구성은 크게 채택된 암호화 알고리듬의 어셈블리 프로그램을 저장할 32K × 24비트 EPROM과 데이타 저장을 위한 8K × 24비트의 RAM, 그리고 DSP56001 칩으로 이루어진다.

하드웨어 보드와 퍼스널 컴퓨터간의 인터페이스에는 RS232C를 사용한 비동기 통신

방법을 사용하였다. 비동기 통신방식에서는 통신 속도, 데이타 길이, 패리티비트, 그리고 스타트 및 스톱비트가 설정되어야 하며, 본 논문에서는 이 값들을 9600bps 혹은 38400bps, 8-bit, no-parity, 1 start-bit, 1 stop-bit 로 하였다.

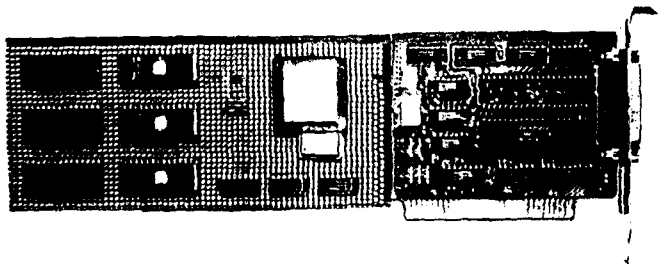

Fig. 3. Plug-in board

V. 실험 및 고찰

개발한 퍼스널 컴퓨터용 관용 암호화 장치를 운용할 소프트웨어는 퍼스널 컴퓨터에 이식시킬 소프트웨어와 DSP56001에 구현시킬 소프트웨어로 구별된다. 퍼스널 컴퓨터에서 암호화에 관련한 명령어 제어, 화일의 입/출력에 관련한 명령어 및 하드웨어와 PC간의 인터페이스를 처리하는 프로그램은 C-언어로 구성하였다. 그림 6 (b)은 본 시스템을 사용하여 (a)의 화일 내용을 암호화한 것이다.

Ⅵ. 결 론

본 논문에서는 관용 암호화 알고리듬을 실시간에 수행하는 퍼스널 컴퓨터용 하드웨어 보드를 제작하고 이 장치를 운용할 소프트웨어를 개발하였다. 채택한 관용 암호화 알고리듬은 Lucifer 알고리듬을 변형시킨 것으로 평문과 암호문의 심볼간 상호 의존도는 DES와 대등하며, Lucifer보다 크게 개선된 것이다. 키이관리에 있어서는 공용 키이 암호 알고리듬을 사용하여 사용자의 두 통신자간의 인증과 세션키이(session key)를 생성 하였다.

하드웨어 보드 제작은 고속 디지틀 신호처리 칩인 DSP56001을 사용하였으며, 특히

이 보드는 기존의 퍼스널 컴퓨터의 회로 수정 없이 입출력 포트에 쉽게 장착되도록 제작되었다. 이러한 퍼스널 컴퓨터용 관용 암호화 시스템의 하드웨어를 구현하여 실험한 결과 만족한 결과를 얻었다.

Displacement	Hex codes															ASCII value
0000(0000)	48	65	72	65	20	69	73	20	61	20	63	6F	6D	6D	75	6E	Here is a commun
0016(0010)	69	63	61	74	69	6F	6E	20	73	79	73	74	65	6D	20	6C	ication system l
0032(0020)	61	62	2E	0D	0A	54	6F	64	61	79	20	69	73	20	6D	6F	ab. Today is mo
0048(0030)	6E	64	61	79	2E	0D	0A	0D	0A	4D	79	20	6E	61	6D	65	nday. My name
0064(0040)	20	69	73	20	42	61	65	6B	20	6B	69	6A	69	6E	2E	0D	is Baek kijin.
0080(0050)	0A	31	32	33	34	35	36	37	38	39	31	30	0D	0A	41	42	12345678910 AB
0096(0060)	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	CDEFGHIJKLMNOPQR
0112(0070)	53	54	55	56	57	58	59	5A	0D	0A	0D	0A	4E	6F	77	20	STUVWXYZ Now
0128(0080)	44	53	50	35	36	30	30	30	20	69	6E	74	65	72	66	61	DSP56000 interfa
0144(0090)	63	65	20	74	65	73	74	21	21	0D	0A	54	45	53	54	20	ce test!! TEST
0160(00A0)	4F	4B	21	21	0D	0A	0D	0A	44	53	50	35	36	30	30	30	OK!! DSP56000
0176(00B0)	20	69	73	20	61	20	76	65	72	79	20	66	61	73	74	20	is a very fast
0192(00C0)	70	72	6F	63	65	73	73	6F	72	2E	0D	0A	44	53	50	35	processor. DSP5
0208(00D0)	36	30	30	30	20	54	45	53	54	20	43	4F	4D	50	4C	45	6000 TEST COMPLE
0224(00E0)	54	45	21	21	1A	1C	74	1C	75	1C	76	1C	77	1C	78	1C	TE!! t u v w x
0240(00F0)	79	1C	7A	1C	7B	1C	7C	1C	7D	1C	7E	1C	7F	1C	80	1C	y z { | } ~ .

(a) Original data

Displacement	Hex codes															ASCII value
0000(0000)	6F	97	AE	92	07	ED	F8	61	D6	1E	82	9C	41	16	25	FD	o a ^ A %
0016(0010)	16	F6	31	F7	9F	ED	09	EB	68	FD	65	4A	C2	66	E4	30	1 h eJ+f 0
0032(0020)	3E	53	FF	45	81	17	23	D1	17	89	57	E6	40	E8	7A	C2	>S E # W @ z+
0048(0030)	EE	AC	3D	A3	BC	45	06	8C	48	7D	29	F8	FB	28	34	C2	= =E H}) (4+
0064(0040)	E3	E6	1D	47	19	72	23	CB	3F	3A	6E	86	FC	F9	E1	C0	Gvr# ?:n +
0080(0050)	C2	98	A7	82	E0	FA	BF	62	FB	C8	3A	EE	F9	6E	12	79	+ +b =: n y
0096(0060)	C4	F8	E4	51	FF	2A	FE	F5	76	E7	9D	52	88	55	EE	C0	- Q * v R U +
0112(0070)	58	52	98	5F	23	DD	73	68	C1	84	F9	69	EE	F7	B4	07	XR _# sh i +
0128(0080)	07	7A	79	5A	D8	68	B0	89	C5	0A	18	38	0C	CF	9A	A0	zyZ h* ^8
0144(0090)	7E	F9	54	2A	7F	12	52	86	F4	C1	2E	C5	87	DE	5F	98	~ T*. R . _
0160(00A0)	69	5B	19	BF	8C	1E	B8	C1	07	7A	79	5A	D8	68	B0	89	i[v+ ^ zyZ h*
0176(00B0)	33	0D	AF	D8	EC	18	68	F8	AC	E7	2A	3D	28	49	AF	F2	3 ^h *=(I
0192(00C0)	52	CA	98	E4	B0	85	FD	9E	66	6C	7F	61	6A	83	51	41	R * fl.aj QA
0208(00D0)	56	A1	8C	7B	CC	83	44	81	F9	0E	B0	A9	EF	12	00	94	V { D *
0224(00E0)	38	74	21	6C	F8	72	F9	2A	75	1E	76	1E	77	1E	78	1E	8t!l r *u^v^w^x^
0240(00F0)	79	1E	7A	1E	7B	1E	7C	1E	7D	1E	7E	1E	7F	1E	80	1E	y^z^{^|^}^~^. ^ ^

(b) encrypted data
Fig. 4. Example data

참 고 문 헌

1. W.Diffie and M.E.Hellman, "New directions in Cryptography," IEEE Trans. on Inform. Theory, vol.IT-22, pp.644-654, Nov. 1976.
2. M.E.Hellman, " An Overview of Public Key Cryptography," IEEE Comm. Society Mag., vol.16, no.6, pp.24-32, Nov. 1978.
3. D.B.Newman, Jr., J.K.Omura, and R.L.Pickholtz, "Public-Key Management for Network Security," IEEE Network Mag., vol.1, no.2, pp.11-16, April 1987.
4. 강해동,이창순,문상재, "Lucifer 형태의 암호화 알고리듬에 관한 연구," 대한전자공학회 논문집, vol.26, No.2, pp.32-39, March 1989.
5. DSP56000/DSP56001 Digital Signal Processor User's Manual, Motorola Inc.
6. R.Rivest, A.Shamir, and L.Adleman, " A Method for obtainging digital signatures and public-key cryptosystems," Comm. ACM, vol.21, no.2, pp.120-126, 1986.