FWHT에 의한 디지틀신호의 비화 방법

A Method of Secreting Digital Signals by FWHT

*김 장 복(Kim, C. B.)

요 약

ISDN에 응용될 수 있는 신호의 비화방식에 대하여 연구되었다. FWHT algorithm을 응용하여, FWHT 계수의 부호를 16자의 password에 의하여 조정함으로써 그 비화성이 3×10^{38}이상 되도록 하였으며 기계어에 의한 module을 최적합하게 작성함으로써 시스템에의 firmware화가 쉽도록 하였으며 시스템을 최소화 할 수 있도록 하였다. printed data에 대한 computer simulation으로 N=128일때의 비화 특성을 보였다.

ABSTRACT

Fast Walsh-Hadamard Transform algorithm is discussed for secreting digital signals in ISDN. 16 characters are used for the password to control the coefficients of FWHT. And it gives above $3x10^{38}$ codes. The FWHT module is presented in machine language. So it is applicable to compact cipher system or firmware system. Computer simulation showed secreting characteristics in printed data for N=128.

*홍익대학교 공과대 전자공학과 교수

Ⅰ. 서 론

미래의 정보 통신 서비스는 ISDN(integrated service for digital network)으로 불리우는 종합 정보 통신망에 의해 이루어질 것으로 예견되고 있다. 이 ISDN은 디지틀 통신망을 토대로 하여 발전하므로 ISDN의 성립을 위해서는 전화망의 디지틀화가 이루어져야 하며, 음성 및 비음성 신호를 동일 통신망에서 처리할 수있는 방식이필요해진다. 또한 ISDN의 발전에 따라 개개인의 많은 정보가 통신망 선로상에 주어질 수 있게 됨으로 개인의 프라이버시가 침해를 받을 수 있어 그 방지책이 필요해진다. 미국에서는 육상회선 전화뿐만 아니라 셀룰러, 마이크로웨이브 및 페이징등을 포함한 무선 전화에까지 프라이버시 보호권을 지니도록 하였다.[1]

Expo/East에서 제기된 산업계의 관심사도 어떻게 정보의 비밀을 유지하느냐 하는 문제였다. 더군다나 전화 상대가 부재시에 미리 정해둔 전화 번호에 의해 음성 축적 센터를 호출하여 자유로이 메시지를 녹음·재생할 수 있는 전언 다이얼 서비스가 개시됨에 따라 정보의 보호 방법이 크게 대두되었다.[2][3]

일반적인 암호화 방법은 음성의 고저를 단위시간당 수백번 반전시키거나 주파수 스펙트럼의 뒤섞음으로 정보를 변형시키는 것이었으나 그 부수되는 시스템이 복잡하고 상대적으로 커짐에 따라 비경제적 요소가 많았다. 따라서 본 논문에서는 고속 walsh-Hadamard변환을 응용하여, 현 통신 시스템에 적합하고 Comput한 비화 장치에 활용할 수있는 알고리즘을 보이고자 하였다.

Ⅱ. 변환 및 비화 방식

PCM신호에 대한 FFT(fast Fourier transform)와 FWHT(fast walsh-Hadamard transform)의 차이점은 엄청나다. 임의의 sample data에 관하여 256-point 변환을 할 경우 FFT보다 FWHT가 적어도 12배이상 빠르다.[4]

이것은 FFT에서의 복소수 연산 대신에 FWHT에서는 단순한 가·감 연산만이 요구되기 때문이다. 이 특성은 hardware구성시 FWHT의 최대 장점이 되기도 한다.

한편 Risch는 point 수 N을 변경함에 따라 walsh 함수, Sinc함수, Zero-orderhold 함수에서의 integral mean sguare error를 비교 연구하였는데, N이 32이상일 때 Walsh함수에서의 i.m.s.e가 가장 작은 값으로 빨리 감소됨을 보이고 있다.[5]

또한 음성 신호를 대상으로 할 경우 현 PCM 신호 체계에서 음성에 stationarity를 유지하도록 128-point 정도가 최대한으로 요구되는 point수이다. 따라서 FWHT를 활용한 비화기는 32-point, 64-point, 그리고 128-point의 변환시스템이면 족하다.

본 논문에서는 연산 algorithm상에 명확성을 주기 위해여 식(1)과 같은 단순한 Hadamard matrix를 변환에 사용하였다.[6]

$$H(u,v)=(-1)^{E} \tag{1}$$

단,

$$E=\sum_{i=0}^{n-1}u_i v_i \tag{2}$$

$$U_{decimal}=(U_{n-1}U_{n-2}\cdots\cdots U_1U_0)_{binary} \tag{3}$$

$$V_{decimal}=(V_{n-1}V_{n-2}\cdots\cdots V_1V_0)_{binary} \tag{4}$$

그리고 비화 방법은 2개 password의 종속관계를 사용하였다. 전체 password는 그림 1과 같이 16자의 길이—숫자, Alphabet 대·소문자, 기타 기호—를 가지며 system operator가 8자, terminal 사용자의 개인 password 8자로 구성된다.

따라서 발생 가능한 Code의 수가 3×10^{28} 이상임으로 비화성은 종래의 주파수 분할 스크램블법에 비

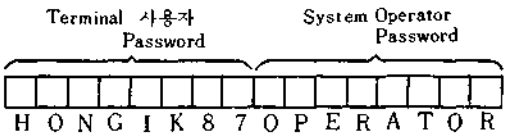

그림 1 Password 규격

하여 비교되지 않을 정도로 크다. 이 방법에 의해 발생할 수있는 개인 password의 총수는 1.7×10^{19} 종류이상이기 때문에 제3자에 의한 우연한 도청은 불가능한 편이다. 비화방식은 주어지는 password에 의해 신호 변환 계수의 부호를 전환하는 방식을 썼다.

FWHT의 변환 algorithm은 그림 2의 flowchart와 같이 구성되었으며 기계어로 작성하여 PROM을 이용한 firmware화가 쉽도록 하였다. 작성된 프로그램의 일례를 부록에 보였다.

Ⅲ. 컴퓨터 모의 실험 및 결과

analog신호의 실험을 위한 기본 시스템은 그림 3

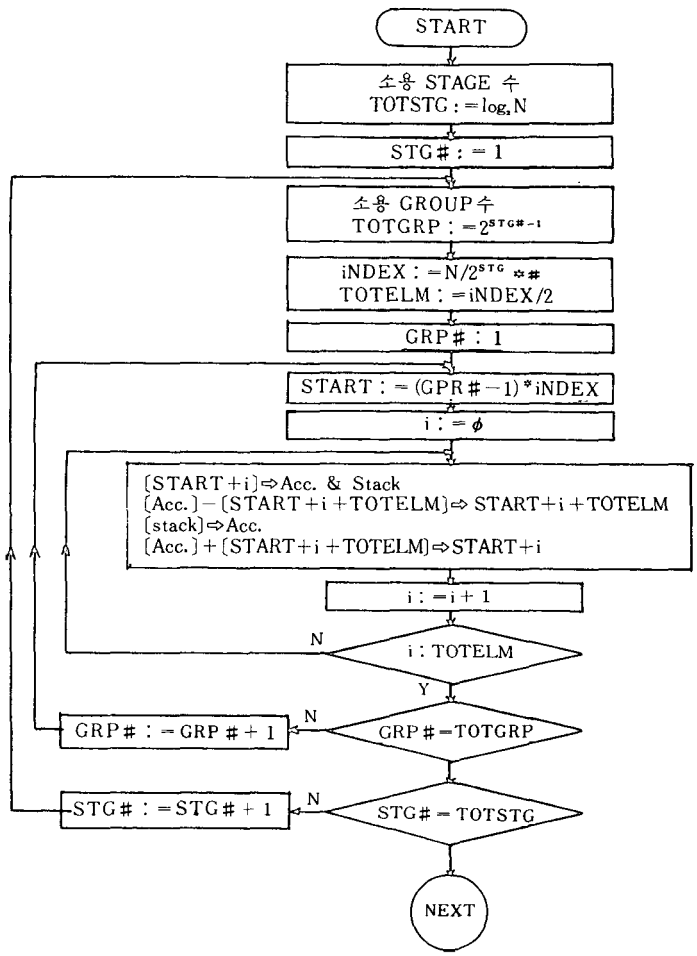

그림 2 FWHT algorithm의 flowchart

과 같으며, 우선 FWHT 프로그램 모듈을 검토하기 위하여 RAM영역에 dump시켜 입·출력 관계를 monitor display로 확인하고, 음성 신호의 처리 관계는 speaker 출력의 hearing test로 확인하였다.

FWHT변환 특성은 음성 신호의 redundancy를 50%로 가정하더라도 128-point에서 40dB이상의 SQNR을 보인다.[7] 좀더 확실한 출력 관계를 구하기 위하여 그림 4 와 같은 printed data처리도에의한 비화 관계를 확인하였는데 그 결과는 그림 5, 그림6과 같다.

원신호로서 그림 5(a), 그림 6(a)와 같은 문장을 입력시키고, 이를 변환·비화시킨 data가 그림 5(a), 그림 6(b)이며, 입력시 사용한 password와 다른 것을 사용하여 복화시킨 것이 그림 5(c), 그림 6(c)이고, 그림 5(d), 그림 6(d)는 제 password를 사용하여 재생됨을 보인 것이다. 랜덤 신호 발생기에서 주어진 data

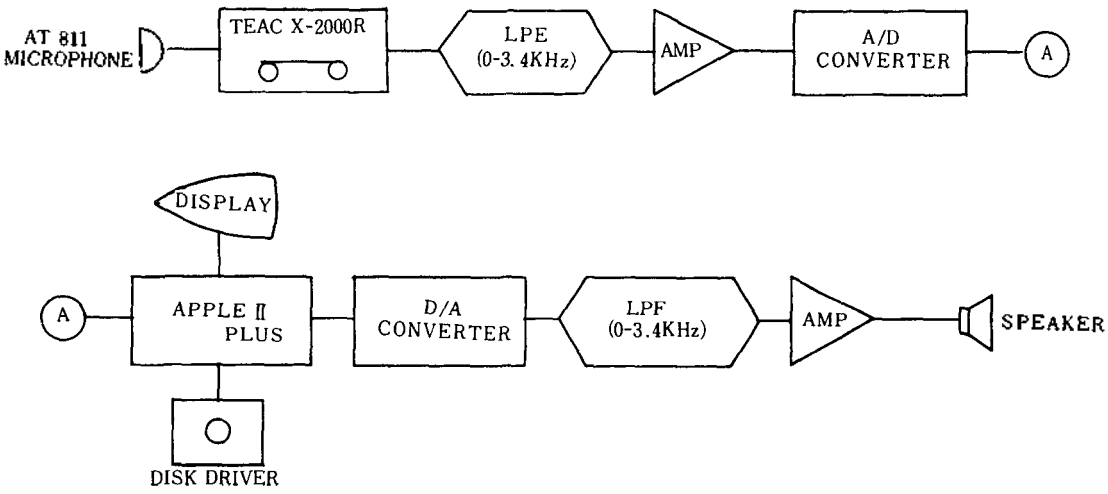

그림 3 기본 모델 시스템

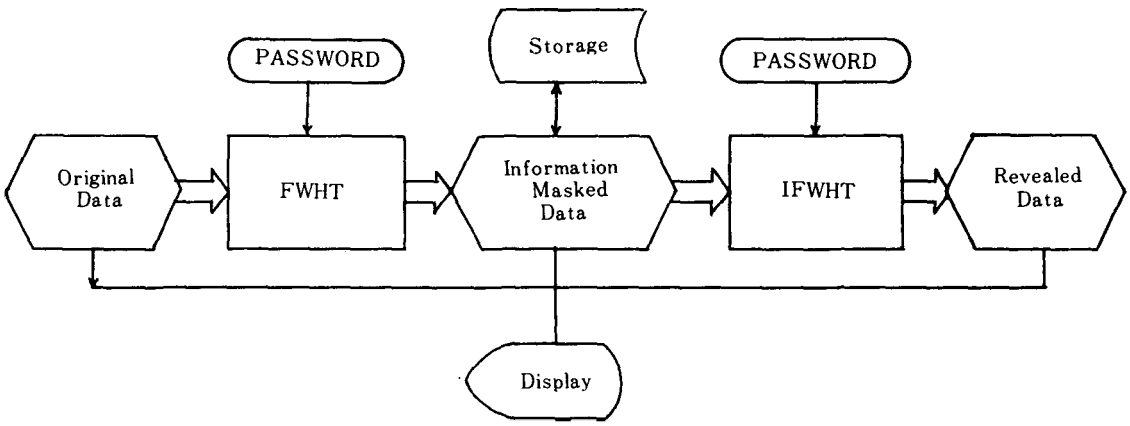

그림 4 printed data 처리개념도

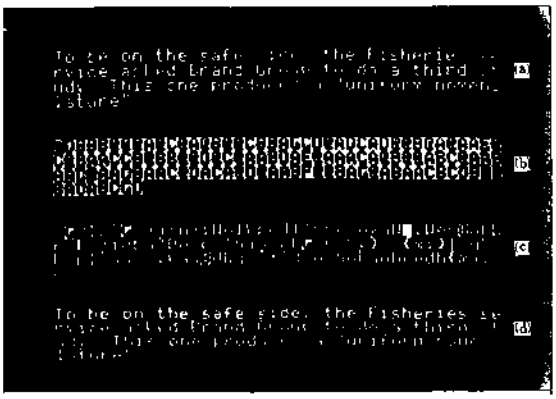

그림 5 printed data의 비화 예 1.
(a) 신신호 원
(b) 변환·비화된 신호
(c) 틀린 password사용 재생신호.
(d) 제 password사용 재생신호.

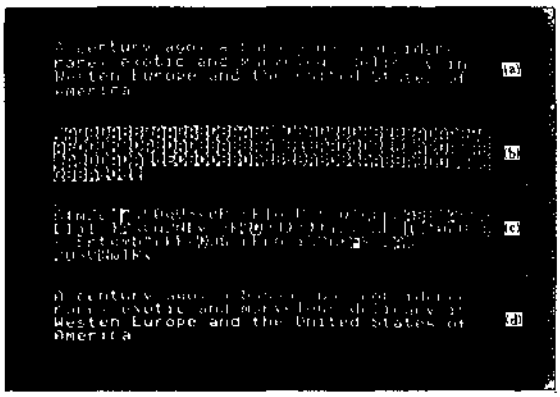

그림 6 printed data의 비화 예 2.
(a) 원 신호
(b) 변환·비화된 신호
(c) 틀린 password사용 재생신호
(d) 제 password사용 재생신호

를 입력으로 삼은 것이 그림 7 이며 그림7(a)는 발생신호, 그림 7(b)는 변환·비화 신호, 그림7(c)는 password가 틀린 경우이고 그림7(d)는 제대로 사용된 경우이다. 원신호에서보다 비화된 신호에서의 상관 관계가 매우 달라짐을 볼 수있다.

모든 실험에 있어서 system operator용 password

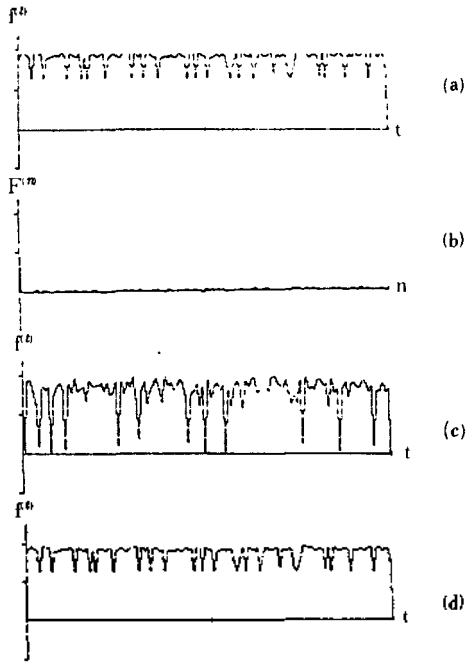

그림 7 random 패턴에 대한 비화
(a) 발생신호
(b) 변환·비화 신호
(c) 틀린 password 사용재생신호
(d) 제password 사용재생신호

는 변경하지 않고 고정시킨 채로, 사용자 password의 변경에 따른 결과만 보인 것이다.

system operator용 password는 main computer의 operator용으로 이용될 수도 있고, terminal 사용자의 second-password로 쓰여 file의 load, save시 password로 사용함으로써 file의 독해뿐만 아니라 저장된 file의 변경후 저장을 방지하도록 할 수 있다. 스크램블을 위한 pseudo-random신호는 shift register방법에 의하여 해결함으로써 모든 시스템의 software화 및 firmware화가 용이하다[8],[9]더구나 shift register의 data form이 Walsh 변환에 별다른 처리 과정의 필요없이 적용될 수 있으므로 system의 compact화에 매우 유리하다.

Ⅳ. 결 론

본 논문에서는 최근 활발한 FFT응용 비화 방식에 필적할만한 FWHT 응용 비화 방식에 대하여 연구하였다. ISDN을 전제로 할 경우 모든 신호가 digital화 될것임으로, binary신호인 경우 software의 algorithm변경 용이, hardware의 firmware화 간편, processing delay의 최소화라는 면에서 FWHT방식이 FFT방식보다 유용할 것임을 제고하였으며, 기제어에 의한 password처리로 개개의 character에 임의의 문자를 모두 사용할 수 있도록 함으로써 16자란 password의 length에 비하여 3×10^{38}이상의 비화도를 갖게 하여 실용성을 지닐 수 있도록 하였다.

그러나 신호의 비화 문제는 시스템 설계자와 시스템 운영정책 입안자가 서로 협조하여야만 소기의 목적을 달성할 수 있으므로 체신 관계자의 검토가 필요하며, 또 현 전화망에 응용될 경우의 신호 동기, signalling등의 문제를 배제하였는데 이는 앞으로 ISDN에서 주어질 신호 처리 방식에 대한 국내 규정의 확립이 우선되어야 할 것임으로 추후 과제로 남아 있다.

부록 FWHT Module

```
1          LST  OFF
2          ORG  $8B00
3          OBJ  $8B00
4  * INITIAL
5          CLD
6          LDY  #$90
7          STY  $07
8          STY  $09
9          DEY
10         STY  $1A
11         STY  $1C
12         DEY
13         STY  $1E
14         STY  $EC
15         LDY  #$00
16         STY  $0305
17         LDA  $0300
18         INY
19         LSR
20         BNE  $8B19
21         STY  $0301
22         INC  $0305
23         LDX  $0305
24         LDA  #$01
25         DEX
26         BEQ  $8B2F
27         ASL
28         JMP  $8B28
29         STA  $0302
30         LDA  $0300
31         LDX  $0305
32         DEX
33         BEQ  $8B3F
34         LSR
35         JMP  $8B38
36         CLC
37         ADC  #$01
38         STA  $0304
39         BEQ  $8B4E
40         LSR
41         STA  $0303
42         JMP  $8B53
43         LDA  #$80
44         STA  $0303
45         LDX  #$00
46         INX
47         TXA
48         PHA
49         LDA  #$00
50         CLC
51         DEX
52         BEQ  $0B64
53         ADC  $0304
54         JMP  $8B5B
55         STA  $06
56         STA  $19
57         STA  $1D
58         ADC  $0303
59         STA  $08
60         STA  $1B
61         STA  $EB
62 *START
63         LDY  #$00
64         LDA  #$00
65         CMP  ($1D),Y
66         BEQ  $8B7E
67         JMP  $8C36
68         CMP  ($EB),Y
69         BNE  $8BDC
70         LDA  ($19),Y
71         CMP  ($1B),Y
72         BCC  $8B85
73         BNE  $8B90
74         LDA  ($06),Y
75         CMP  ($08),Y
76         BCC  $8B85
77         LDA  #$00
78         STA  ($1D),Y
79         STA  ($EB),Y
80         LDA  ($19),Y
81         PHA
82         LDA  ($06),Y
83         PHA
84         CLC
85         ADC  ($08),Y
86         STA  ($06),Y
87         LDA  ($19),Y
88         ADC  ($1B),Y
89         STA  ($19),Y
90         PLA
91         SEC
92         SBC  ($08),Y
93         STA  ($08),Y
94         PLA
95         SBC  ($1B),Y
96         STA  ($1B),Y
97         JMP  $8CEE
98         LDA  #$00
99         STA  ($1D),Y
100        LDA  #$FF
101        STA  ($EB),Y
102        LDA  ($1D),Y
103        PHA
104        LDA  ($08),Y
105        PHA
106        SEC
107        SBC  ($06),Y
108        STA  ($08),Y
109        LDA  ($1B),Y
110        SBC  ($17),Y
111        STA  ($1B),Y
112        PLA
113        CLC
114        ADC  ($06),Y
115        STA  ($06),Y
116        PLA
117        ADC  ($19),Y
118        STA  ($19),Y
119        JMP  $8CEE
120        LDA  ($19),Y
```

```
121             CMP   ($1B),Y
122             BCC   $8C0F
123             BNE   $8BEA
124             LDA   ($06),Y
125             CMP   ($08),Y
126             BCC   $8C0F
127             LDA   #$00
128             STA   ($1D),Y
129             STA   ($EB),Y
130             LDA   ($19),Y
131             PHA
132             LDA   ($06),Y
133             PHA
134             SEC
135             SBC   ($08),Y
136             STA   ($06),Y
137             LDA   ($19),Y
138             SBC   ($1B),Y
139             STA   ($19),Y
140             PLA
141             CLC
142             ADC   ($08),Y
143             STA   ($08),Y
144             PLA
145             ADC   ($1B),Y
146             STA   ($1B),Y
147             JMP   $8CEE
148 ***********
149             LDA   #$FF
150             STA   ($1D),Y
151             LDA   #$00
152             STA   ($EB),Y
153             LDA   ($1B),Y
154             PHA
155             LDA   ($08),Y
156             PHA
157             CLC
158             ADC   ($06),Y
159             STA   ($08),Y
160             LDA   ($1B),Y
161             ADC   ($19),Y
162             STA   ($1B),Y
163             PLA
164             SEC
165             SBC   ($06),Y
166             STA   ($06),Y
167             PLA
168             SBC   ($19),Y
169             STA   ($19),Y
170             JMP   $8CEE
171 **********
172             LDA   #$00
173             CMP   ($EB),Y
174             BNE   $8C97
175             SEC
176             LDA   ($19),Y
177             CMP   ($1B),Y
178             BCC   $8C70
179             BNE   $8C4B
180             LDA   ($06),Y
181             CMP   ($08),Y
182             BCC   $8C70
183             LDA   #$FF
184             STA   ($1D),Y
185             STA   ($EB),Y
186             LDA   ($19),Y
187             PHA
188             LDA   ($06),Y
189             PHA
190             SEC
191             SBC   ($08),Y
192             STA   ($06),Y
193             LDA   ($19),Y
194             SBC   ($1B),Y
195             STA   ($19),Y
196             PLA
197             CLC
198             ADC   ($08),Y
199             STA   ($08),Y
200             PLA
249             SEC
250             SBC   ($08),Y
201             ADC   ($1B),Y
202             STA   ($1B),Y
203             JMP   $8CEE
204 *******
205             LDA   #$00
206             STA   ($1D),Y
207             LDA   #$FF
208             STA   ($EB),Y
209             LDA   ($1B),Y
210             PHA
211             LDA   ($08),Y
212             PHA
213             CLC
214             ADC   ($06),Y
215             STA   ($08),Y
216             LDA   ($1B),Y
217             ADC   ($19),Y
218             STA   ($1B),Y
219             PLA
220             SEC
221             SBC   ($06),Y
222             STA   ($06),Y
223             PLA
224             SBC   ($19),Y
225             STA   ($19),Y
226             JMP   $8CEE
227 ******
228             LDA   ($19),Y
229             CMP   ($1B),Y
230             BCC   $8CCA
231             BNE   $8CA5
232             LDA   ($06),Y
233             CMP   ($08),Y
234             BCC   $8CCA
235             LDA   #$FF
236             STA   ($1D),Y
237             STA   ($EB),Y
238             LDA   ($19),Y
239             PHA
240             LDA   ($06),Y
241             PHA
242             CLC
243             ADC   ($08),Y
244             STA   ($06),Y
245             LDA   ($19),Y
246             ADC   ($1B),Y
247             STA   ($19),Y
248             PLA
251             STA   ($08),Y
252             PLA
253             SBC   ($1B),Y
254             STA   ($1B),Y
255             JMP   $8CEE
256 ******
257             LDA   #$FF
258             STA   ($1D),Y
259             LDA   #$00
260             STA   ($EB),Y
261             LDA   ($1B),Y
262             PHA
263             LDA   ($08),Y
264             PHA
265             SEC
266             SBC   ($06),Y
267             STA   ($08),Y
268             LDA   ($1B),Y
269             SBC   ($19),Y
270             STA   ($1B),Y
271             PLA
272             CLC
273             ADC   ($06),Y
274             STA   ($06),Y
275             PLA
276             ADC   ($19),Y
277             STA   ($19),Y
278             INY
279             CPY   $303
280             BEQ   $8CF7
281             JMP   $8B75
282             PLA
283             TAX
284             CPX   $302
285             BEQ   $8D01
286             JMP   $8B55
287             LDA   $305
288             CMP   $301
289             BEQ   $8D0C
290             JMP   $8B20
291             RTS
```

參 考 文 獻

1. 미상원 분과위원회, 통신 프라이버시법 통과, TIS-86-38, 1986
2. 음성 비화기 소형소자, TIS-86-9, 1986
3. 고도 정보 사회의 Security, TIS-86-14, 1986.
4. 오광우, "어셈블리어에 의한 256점 FWHT와 FFT의 변환특성 비교에 관한연구," 홍익대, 석사학위논문, 1986. 11.
5. Risch, P.R., "Evaluation of Data Reconstruction using Walsh Functions," Elect. Lett. Vol.9: 21, pp.489-490, 1973.
6. Ahmed, N. and Rao, K.R., *Orthogonal Transform for the Digital Signal Processing*, Springer-Verlag, 1975.
7. 김장복, "한글음성신호의 리얼타임 인식을 위한 Walsh변환에 의한 코딩특성에 관한연구," 연세대, 박사학위 논문, 1983. 6.
8. 이근영, "쉬프트 레지스터를 사용한 순서회로의 최적실 실현," 한양대, 박사학위 논문, 1987. 7.
9. Golomb, S.W., *Shift Register Sequences*, Holden-Day, 1967.
10. Rao, K.R., *Discrete Transforms and Their Applications*, Van N.R., 1985.