동기식 정보보호시스템 분석

염 흥 열*, 김 춘 수**, 이 홍 섭**
순천향대학교 전자공학과*, 한국전자통신연구소**

Analysis on the Secure SDH Multiplexer

Heung-Youl, Youm*, Choon-Soo, Kim**, Hong-Sub, Lee**
Dept. of Electronics Eng. Soonchunhyang Univ.*
Electronics & Telecommunications Research Institute**

- 요약 -

본 고에서는 기존의 동기식 전송망과 다중시스템의 구조를 분석하고, 이를 바탕으로 동기식 다중 시스템에 정보보호 서비스를 부가한 동기식 정보보호 시스템을 위한 요구 사항, 정보보호 서비스, 그리고 서비스를 실현하기 위해 요구되는 정보보호 메카니즘 등을 제시한다. 제시된 정보보호 메니즘은 정보보호 시스템을 위한 요구 사항을 만족하므로 동기식 정보보호 시스템 실현시 유용하게 활용될 수 있다. 또한 동기식 정보보호 시스템을 실현하기 위한 세부 구성도를 제안하고 관련 부분의 기능을 구체적으로 제시한다. 제안된 구조는 기존의 동기식 다중 시스템과 호환성이 있게 연동될 수 있고 기존의 동기식 다중시스템에 최소로 변경하여 실현될 수 있음을 확인한다. 그리고 RSA 와 MD5 알고리즘을 이용한 공개키 증명서를 C 언어로 실현하고 이를 시뮬레이션한다. 시뮬레이션 결과 공개키 증명서가 동기식 정보보호시스템에서 요구되는 성능을 만족함을 확인한다.

1. 서 론

동기식 정보보호 시스템은 동기식 다중 시스템에 정보보호 기능을 부가한 동기식 시스템의 일종이다. 지금까지 비동기식 전송 방식으로 실현되던 전송망은 ITU 의 G.70X 의 동기식 디지털 계위를 바탕으로 하는 동기식 전송망으로 진화될 예정이다.[1,2,3,4,5,6,7]

ATM 통신기술과 SDH 전송망을 바탕으로 구성될 광대역 ISDN은 국간 전송망에서의 기본 전송 단위 신호로 SDH 의 STM-1 신호를 채용하고 있다. 미국의 사이링스사에서는 SONET 용 동기식 정보보호 시스템을 일부 개발한 바 있고, 미국의 DEC사에서는 STM-1 신호에 적용 가능한 속도를 갖는 DES 정보보호 칩을 개발한 바 있다. 우리 나라에서도 STM-1 신호의 동기식 다중 시스템이 개발되어 국내망에 설치될 예정이다. 그러나 국내 STM-1 동기식 다중 시스템에서는 정보보호 기능이 고려되어 있지 않다. 해커에 의한 전산망의 파괴, 정보도용 및 변조가 급증하고 있는

추세를 고려하면, 기간 전송망에서의 정보 보호는 시급히 요구되어 지고 있다. 또한 광대역 ISDN 신호의 전송 신호 단위인 ATM 셀은 국간 전송 및 UNI(User Network Interface) 에서 STM-1 다중 구조하의 페이로드를 이용한다. STM-1 신호가 운반하는 정보는 다양한 유형의 데이타, 디지털 화된 음성 및 비디오 신호가 될 것이다. 따라서 STM-1 신호용 다중 시스템의 이용은 광대역 ISDN이 확대됨에 따라 활용이 증대될 것이며, 이에 대한 정보보호 시스템도 활용이 증대될 것이다.

본 고에서는 동기식 정보보호 시스템을 실현하기 위하여 기존의 동기식 전송망과 다중 시스템의 구조를 분석하고, 이를 바탕으로 동기식 다중시스템에 정보보호 서비스를 부가한 정보보호 시스템을 위한 요구 사항과 정보보호 서비스, 그리고 서비스를 실현하기 위해 요구되는 정보보호 메카니즘을 제시한다. 또한 동기식 정보보호 시스템을 실현하기 위한 세부 구성도를 제안하고 관련 부분의 기능을 구체적으로 제시한다. 또한 동기식 정보보호 시스템에 적용 가능한 구체적인 정보보호 알고리즘을 제시한다. 그리고 RSA 와 MD5 알고리즘을 이용한 공개키 증명서를 C 언어를 이용하여 실현하고 이를 시뮬레이션한다.

2. 본론

2.1 동기식 다중 시스템

동기식 다중 시스템인 SDH (Synchronous Digital Hierarchy) 시스템의 외부 인터페이스는 동기식 다중 계위의 기본 신호인 STM-N (Synchronous Transfer Module - level N) 신호, 기존의 비동기식 전송망의 기본 계위 신호인 G.703 신호, 망 관리 및 운용을 위한 TMN (Telecommunication Management Network) 과의 접속을 위한 Q 인터페이스와 동기식 전송망의 운용 및 관리 채널인 DCC (Data Communication Channel) 과 유지보수 요원과 동기식 시스템간의 F 인터페이스, 그리고 SDH 시스템의 망동기를 위한 동기 인터페이스 등으로 구성된다.[5,6,7]

SDH 시스템은 그림 2.1과 같은 SDH 신호 다중 구조에 바탕을 두고 구성된다.

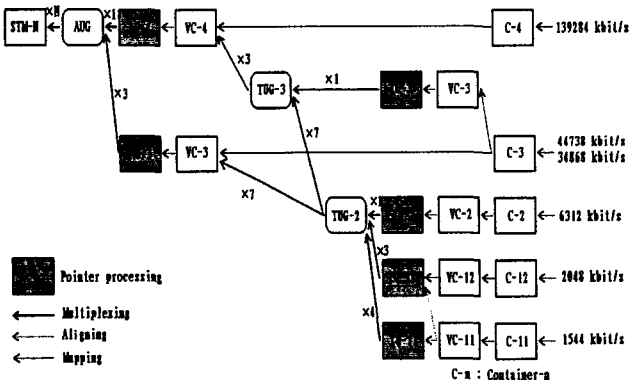

그림 2.1 SDH 신호 다중 구조

SDH 시스템의 일반적인 논리적 블럭도(Logical Block Diagram) 는 그림 2.2와 같다.

G.703 신호에서 STM-N 신호로의 다중은 두 경로로 분류되어 실현된다. 하나는 DS4 급 이상의 신호를 하나의 사상(Mapping) 단계를 거쳐 STM-N 신호로 다중화 하는 경로이고, 다른 하나는 DS3 급 이하의 신호들을 두번 이상의 사상 단계를 거쳐 STM-N 신호로 다중화 하는 경로이다.

종속 신호(Tributary Signal) 들의 STM-N 신호로의 사상은 다음과 같은 과정으로 수행된다. PPI (PDH Physical Interface) 와 LPA(Lower order Path Adaptation) 는 기존의 DS1, DS2, DS3, 그리고 DS4 등의 G.703 PDH(Plesiochronous Digital Hierarchy) 신호와 인터페이스하여 동기식 Container 신호들 (C-11/12/2/3/4) 을 생성한다. LPT (Lower order Path Termination) 는 C-11/12/2/3 에 VC-11/12/2/3 POH (Path OverHead) 을 부가하여 VC-11/12/2/3 신호를 생성한다. LPC(Lower order Path Connection) 는 특정의 VC-11/12/2/3 신호가 하드웨어 구성 양태에 따라 VC-3/4 내의 특정 타임스롯으로 할당되는 것을 방지하고 VC-3/4 내의 임의의 타임스롯으로 할당되도록 한다. 이는 타임슬롯 교환 회로를 이용하여 실현될 수 있다. LUG(Lower order path Unequipped Generator) 는 현재 연결(Connection) 이 할당되어 있지 않은 경로(Path) 에 unequipped signal Label 을 갖는 유효한 VC-1/2 신호를 전송함으로서 연결의 성능을 감시한다. HOA(Higher Order path Adaptation) 는 VC-11/12/2/3 에 각각의 TU 포인터를 부가하고, 이들 신호를 합성하여 C-3/4 신호를 생성한다. HPT(Higher order Path Termination) 은 C-3/4 신호에 VC3/4 POH를 부가하여 VC3/4 를 생성한다. HPC(Higher order Path Connection) 는 특정의 VC-3/4 의 STM-N 신호로의 능동적인 상호 연결 (Flexible Connection) 을 가능케 한다. HUG(Higher order path Unequipped Generator) 는 사용치 않고 있는 HO(Higher Order) 연결 (Connection) 에 대하여 Unequipped Signal 레벨(Label) 을 갖는 유효한 VC-3/4 을 생성하고 감시하는 기능을 수행한다.

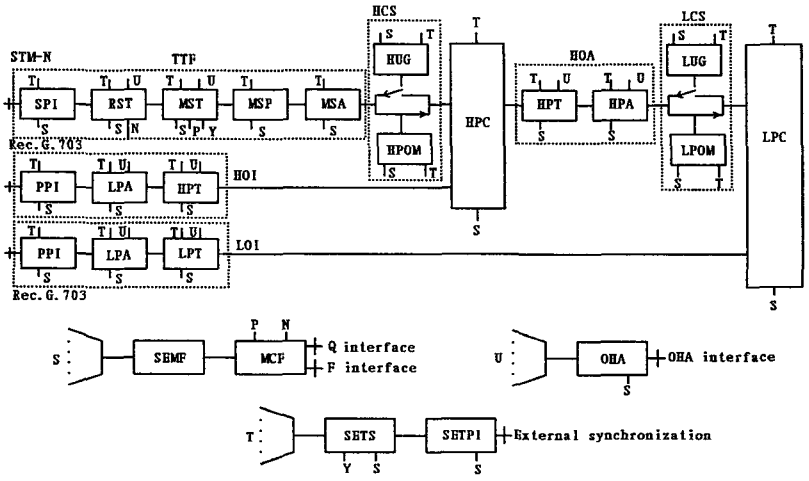

그림 2.2 SDH 시스템의 일반적인 논리적 블럭도

MSA(Multiplex Section Adaptation) 은 VC-3/4 에 AU-3/4 포인터를 부가하고, 여러 개의 AU-3/4(Administration Unit-3/4) 들을 모아서 생성된 AUG(Administration Unit Group) 를 바이트 인터리빙(Byte Interleaving) 하여 구간 오버헤드 (Section Overhead) 를 뺀 나머지 STM-N 신호를 생성한다. MST(Multiplex Section Termination) 는 STM-N SOH 중 5열에서 8열까지의 MSOH(Multiplex Section Overhead) 를 부가한다. RST(Regenerator Section Termination) 는 1열에서 3열까지의 RSOH(Regenerator Section Overhead) 를 삽입하는 기능과 수신 광신호로 부터 클럭의 복구를 용이케하는 스크램블링(Scrambling) 기능을 갖는다. SPI(SDH Physical Interface) 는 논리 레벨 STM-N 신호를 STM-N 인터페이스 신호로 변환하는 기능을 수행한다.

한편, STM-N 신호에서 G.703 신호로의 역다중은 이의 반대 기능을 수행한다. SPI 는 STM-N 인터페이스 신호에서 논리 레벨 신호로 변환하는 기능을, RST는 프레임 동기, 역스크램블링, 그리고 수신 RSOH 처리 기능을 수행한다. HPOM(Higher order Path Overhead Monitor) 은 송신 HUG 와 쌍을 이루어 연결이 할당되지 않은 VC-3/4 경로에 대한 성능을 감시한다. LPOM(Lower order Path Overhead Monitor) 역시 LUG 와 쌍을 이루어 연결이 설정되지 않은 VC-11/12/2/3 을 감시한다.

예를 들어, 북미 방식 DS1 신호가 STM-N 신호로 사상되는 과정은 다음과 같다. PPI 와 LPA 는 DS1 신호를 C-11 신호로 변환하고, LPT 는 VC-11 POH 를 부가하여 VC-11 신호를 생성하며, LPA와 LPT는 여러개의 VC-11 들을 모으고 각각에 TU 포인터를 부가하여 VC-3 신호를 생성한다. 그리고 MSA는 VC-3 신호들을 모으고 각각에 AU 포인터를 부가하여 SOH를 뺀 STM-N 신호를 생성하고, MST는 여기에 MSOH 를 부가하며, RST는 여기에 RSOH 를 부가하여 STM-N 신호를 생성하고, SPI 는 STM-N 인터페이스 신호를 생성한다.

SDH 시스템의 TMN 인터페이스는 동기식 전송망의 관리를 위한 TMN 정보를 전달하는 DCC (Data Communications Channel), 기존의 X.25 망을 통해 SDH 시스템과 TMN 의 OS (Operating System) 을 연결하는 Q 인터페이스 등이 있다. DCC 는 중계기나 다른 망요소에서 액세스가 가능한 D1-D3 바이트와 다중 시스템에서만 액세스 가능한 MSOH 내의 D4-D12 바이트로 구성되어 있다. DCC 채널은 메시지-기반 프로토콜(Message-Oriented Protocol) 을 이용하며, 동기식 망요소 간의 유지보수를 위한 통신 채널로 이용된다. Q 인터페이스는 SDH 시스템과 TMN 과의 인터페이스를 위하여 기존의 데이타 통신망을 이용하여 실현된다.

단말과 중계기간의 선형 구조(Linear System Configuration) 로 실현된 DCC 채널의 이용은 그림 2.3과 같다. 단말과 중계기간의 트리 구조(Tree Configuration) 로 실현된 DCC 채널의 이용은 그림 2.4와 같다.

그림 2.4 의 SEMF (Synchronous Equipment Management Function) 는 SDH 시스템에서 발생되는 성능 감시 데이타와 여러 종류의 하드웨어 경보를 SDH 시스템내의 S 인터페이스를 통해 수집하고, 이들을 객체 지향(Object-Oriented) 메시지로 변환하여, 이를 DCC 나 Q 인테페이스를 통해 OS 로 전송하기 위하여 MCF (Message Communication Function) 로 전달하는 기능과, OS 로 부터 수신한 유지보수 관련 명령을 시스템내의 Sn 기준점을 통해 각 기능 블럭으로 전달하는 기능을 수행한다. MCF 는 SEMF 에 의하여 시스템내의 Sn 인터페이스를 통해 수집된 유지보수

정보를 DCC, Q, 그리고 F 인터페이스에 적합한 메시지로 변환하고, DCC, Q, F 인터페이스를 통해 수신된 메시지를 저장하며, DCC 를 통해 입력된 메시지가 자국의 메시지가 아닌 경우 이를 다른 망요소로 경로배정(Routing) 한다.

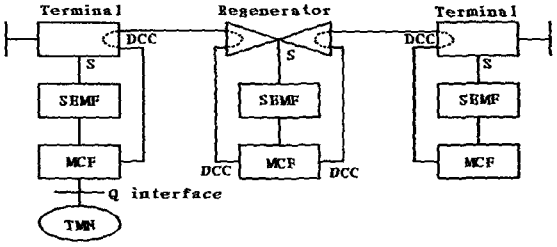

그림 2.3 단말과 중계기간의 선형 구조로 실현된 DCC 채널의 이용

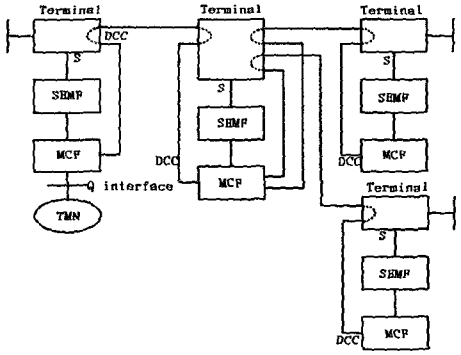

그림 2.4 단말과 중계기간의 선형 구조로 실현된 DCC 채널의 이용

망요소는 미래의 새로운 서비스 수요에 대처하고 하나의 연결에 대한 대체 경로를 설정하기 위하여, 연결이 할당되어 있지 않은 경로나 전체 경로의 일부분인 불완전 경로 구간 (Incomplete Path Segment) 의 성능을 감시해야 한다. 성능 감시는 하나의 연결에 하나 이상의 대체 경로 (Alternative Path) 를 미리 설정하고, 서비스를 제공하고 있는 경로에 장애가 발생했을 경우 즉시 대체 경로를 통해 서비스를 제공함으로서 장애 복구 시간을 감소할 수 있기 위하여 수행된다. 이는 Unequipped 신호 레벨을 갖는 VC 를 생성하는 HUG 와 수신된 경로 오버헤드를 이용하여 해당 경로에 대한 성능을 감시하는 HPOM 으로 구성되는 HCS(Higher order Connection Supervision) 을 이용하여 실현된다.

E1/E2 바이트를 이용하는 타합선 (Order-Wire) 기능은 요지보수 요원이 이용하는 중계기 및 다중 시스템간의 음성 채널로 이용된다. E1 바이트는 중계기에서 액세스가 가능하며, E2 바이트는 다중 터미널에서만 액세스가 가능한 음성채널이다.

사용자 채널인 F1 바이트는 중계기와 다중 단말(Multiplex Terminal) 에서 액세스될 수 있다.

2.2 동기식 다중시스템을 위한 요구 사항 및 서비스

동기식 정보보호시스템을 위한 요구 사항은 다음과 같다.

① 정보보호 서비스를 부가한 동기식 신호는 기존의 동기식 전송망을 통해 전송될 수 있어야 한다.

② 동기식 전송망이 회선분배시스템, 다중시스템, 그리고 Add-Drop 시스템으로 구성되어 있음을 고려하여 동기식 신호의 정보보호는 동기식 신호의 생성점에서 종단점까지의 모든 동기식 전송망을 통한 경로(Path) 구간에 대하여 수행되어야 한다.

③ 기밀성 서비스를 위한 스크램블러의 안전성은 적어도 DES 정도의 안전성을 가져야 한다.

④ 정보보호 서비스의 부가로 인해 요구되는 기능은 최소화되도록 구성되어야 한다.

⑤ 기밀성 서비스를 제공하기 위한 기밀성 알고리즘은 최소로 155Mbps 정도의 동기식 신호를 처리할 수 있어야 한다.

⑥ 정보보호 서비스는 이식성과 편리성이 있어야 한다.

⑦ 동기식 정보보호시스템은 기존의 동기식 다중시스템과 호환성을 이룰 수 있도록 ITU 권고안을 충분히 반영해 설계되어야 한다.

⑧ 키 분배 및 인증을 위한 비밀 정보는 안전하게 보관되어야 한다. 따라서 스마트 카드 형태로 이 정보들은 보관되어야 한다.

동기식 정보보호시스템에서 요구되는 정보보호 서비스는 동기식 페이로드 신호 보호를 위한 기밀성 서비스, 기밀성 서비스를 위한 키 분배 서비스, 그리고 키 분배시 상대방의 정체를 확인하기 위한 개체 인증 서비스 등으로 구분된다. [9,10,11,12,14,16]

2.3 정보보호 구간 및 정보보호 방식 제안

동기식 정보보호 시스템은 고속의 기밀성 서비스를 제공해야 한다. 동기식 정보보호시스템에 적용될 수 있는 정보보호 방식은 선형 복잡도가 충분히 큰 스트림 정보보호 방식을 이용하는 방식과 DES 또는 IDEA 를 스트림 방식으로 이용하는 OFB(Output FeedBack) 모드가 고려될 수 있다.

스트림 방식에 대한 정보보호 알고리즘의 동기는 VC 의 POH 중 여분의 POH 을 이용하여 실현한다. 정보보호 알고리즘의 동기 손실 여부 판단은 현재 이용되고 있지 않은 POH 에 특정 패턴을 전송한 후, 수신단에서 이를 검출함으로서 정보보호 알고리즘의 동기 여부를 결정할 수 있다.

인증 및 키 분배를 위한 채널로는 VC-POH 의 F2 바이트를 이용한다. 이의 생성 및 종단은 OHA(OverHead Access) 이므로 OHA는 키 분배 및 인증 기능에 관여해야 한다.

스크램블러를 위한 키의 갱신은 수초 또는 수분 단위로 수행되어야 한다.

상대방의 인증은 최초 통신 개시 및 일정 주기로 수행되어야 한다. 세션키 분배는 통신 쌍방의 협조로 수행되어야 한다.

보호 신호의 단위는 STM-N 의 페이로드부, VC3 의 C3, VC4 의 C4, 또는 VC-1/2 의 C-1/2 들 이다.

동기식 정보보호 시스템을 위한 망 관리는 단기적으로는 동기식 정보보호 시스템만을 관리하는 별도의 망관리 시스템을 이용하여 실현되어야 하며, 장기적으로는 TMN 과의 정보 교환을 통해 이루어져야 한다. 이는 TMN 인터페이스를 통해 수행된다.

X.509에서 요구되는 공개키 증명서 (Certificate) 의 발급을 위하여 모든 동기식 정보보호 시스템이 믿을 수 있는 제삼자인 TTP (Trusted Third Party) 을 요구하며, 공개키 증명서에 의한 인증 및 키 분배 기능을 실현할 수 있다. 망 관리 시스템과 동기식 망요소와의 망정보 교환시 요구되는 보호 서비스는 요구되는 계층과 관련 계층에 대한 보호연관 (Security Association) 의 설정 방법, 각 계층이 SMIB(Security Management Information Base) 을 구축하는 방법과 보호연관의 속성을 규명할 필요가 있다. 키 분배 및 인증을 위하여 스마트카드를 이용한다.

2.4 정보보호 시스템의 구조 및 정보보호 알고리즘

동기식 정보보호 시스템에서 요구되는 정보보호 서비스는 정보보호 메카니즘들에 의해 실현되어야 한다. 기밀성 서비스를 위한 정보보호 메카니즘은 Triple DES, IDEA 또는 DES 의 CBC 모드, 그리고 DES 와 IDEA 의 OFB 모드가 고려될 수 있다. [16, 20]

인증 및 키 분배는 ITU X.509 의 인증 프로토콜을 이용하며, 인증 방식은 ITU X.509 에서 권고하고 있는 강력 인증 방식중의 하나인 일회, 이회, 또는 삼회 인증 방식을 적용한다.[8,9,10,13,18,19]

스크램블러를 위한 키 분배는 인증 정보의 교환시에 이용되는 데이타 토큰을 이용하여 실현하며, ISO 에서 표준화되고 있는 키 분배 방식을 적용한다.

2.5 동기식 정보보호시스템 구조

동기식 정보보호 시스템도 동기식 다중시스템의 한 종류로서 기본적으로 2.1 절에서 제시된 기본 블럭도를 이용하여 실현될 것이다. 본 절에서는 동기식 정보보호 시스템 설계시 기존의 동기식 다중시스템의 구조에서 변경이 요구되는 기본 블럭 만을 도출하여 그 기본 블럭을 제시한다. 변경이 요구되는 기본 블럭은 LPT 또는 HPT, OHA, 그리고 SEMF 등이다.

가. HPT 및 LPT 구조

VC3/4 신호는 HPT (Higher order Path Termination) 또는 LPT 에 의해 구성된다. 정보보호 구간이 경로가 생성되고 종단되는 점까지의 모든 경로 구간을 포함하므로 기밀성 서비스 제공을 위한 스크램블러의 위치는 LPT 의 입력점이 될 것이다. VC3/4 신호는 기존의 POH(Path OverHead) 를 이용하여 실현되어야 한다. VC3/4 POH 는 다음과 같은 종류로 구분될 수 있다.

- 종점간의 통신을 위한 POH : J1, B3, C2, G1, K1(bit 1-4)
- 페이로드 유형을 구분하는 POH : H4, F2, F3

- 미래 국제 표준을 위해 유보된 POH : K3(bit 5-8)
- 운용 영역에서 이용되는 POH : N1

J1 바이트는 수신국이 통신을 수행하고 있는 동안에 원래의 송신국과 계속 연결되어 있다는 것을 확인하기 위한 경로 추적 (Path Trace) 바이트이다. B3 바이트는 오류 감시를 위해 할당되었으며, BIP-8 부호를 이용하여 생성되고 검출된다. C2 바이트는 VC3/4 신호의 구성 형태를 나타내는 신호 레벨을 나타낸다. G1 바이트는 경로 생성원에서 수신단까지의 경로에 대한 성능감시 결과를 상대국에 되돌려 주기 위한 REI(Remote Error Indication) 부와 자신의 장애 및 결함 상태를 상대국에 전달하기 위한 RDI(Remote Defect Indication) 부로 구분된다. F2, F3 바이트는 경로 사용자 채널로서, 경로 사용자가 별도로 사용하는 채널이다. H4 바이트는 VC1/2 신호를 위한 다중 프레임 위치 표시자로서 이용된다. K3 바이트중 비트 1-4는 VC3/4 의 자동 보호 절체 기능의 실현을 위한 바이트이다. N1 바이트는 망 운용자 용으로, TCM(Tandem Connection Monitoring) 용으로 할당되었다.

스크램블링 알고리즘은 기밀성 메카니즘을 이용하며, 적어도 DES 이상의 안전성이 있도록 설계되어야 한다. F2 바이트를 위한 키 분배는 기밀성 서비스의 안전성을 고려하여 충분히 빠른 간격으로 변경되어야 한다. 스크램블러에서 충분한 키 변경 시간을 보장하기 위하여 스크램블러의 키는 2개의 키를 사용한다. 이들은 우수 관용키와 기수 관용키라 명명된다.

정보보호 시스템이 정보보호 서비스를 위하여 이용해야 할 POH 채널은 경로 사용자 채널인 F2와 F3 바이트이다. F2 바이트는 프로토콜 기본 메시지 기반 데이타 통신 채널로서 Q.921 LAPD 데이타 링크 프로토콜을 이용한다. F2 바이트는 키 분배 및 인증 채널로 이용된다. F3 바이트는 그림 2.5 와 같이 스크램블러의 동기를 위한 7비트와 나머지 블럭 정보보호 알고리즘이 이용되는 것을 대비한 멀티프레임 동기를 위한 1 비트로 구성된다. F3 바이트는 스트림 방식을 이용하는 경우 정보보호 알고리즘용 동기 바이트를 위해 설정되었다. F3 바이트는 실제로 교환되는 새로운 세션키를 스크램블러 또는 디스크램블러에 로드하는데 이용된다. 정상 상태에서의 F3 바이트의 비트 1-7 은 "0000000" 로 부호화되며, 상대방에게 키 변경을 알리기 위하여 일정 횟수 (예, 4) 프레임 동안 비트 1-7 을 "1111111" 로 부호화하여 전송한다. 이는 3 개의 오류 정정 능력이 있는 반복 부호이다.

정보보호 알고리듬 동기용 7 비트	블럭 암호 알고리듬 동기용 1 비트

그림 2.5 F3 바이트의 할당

C4 신호의 POH 를 제외한 바이트 수는 2340 바이트로서 8 바이트 단위로 동작하는 블럭 알고리즘과 동기를 이룰 수 없다. 따라서 2 개의 프레임을 구성하면 4680 바이트가 되어 8 바이트의 배수가 된다. 따라서 비트 8 은 '1' 과 '0' 이 반복되는 패턴을 가질 것이다.

기밀성 메카니즘이 적용되는 신호의 범위는 그림 2.6과 같이 POH 를 제외한 전체 VC3/4 신호가

될 것이다.

정보보호 알고리즘의 동기가 어긋나면 정보보호 시스템은 정상적인 동작을 할 수 없다. 각 페이로드는 고정적인 비트로 할당되며 동기식 전송망의 여타의 망요소에서 변경되지 않는 R 비트를 반드시 갖고 있다. 동기식 정보보호 시스템의 송신단은 이 R 비트를 특정 패턴으로 셋하여 전송하고, 수신단에서는 이 R 비트 패턴이 전송된 R 비트 패턴과 일치하는가를 검사한다. 검사 결과, 같으면 정보보호 알고리즘의 동기가 이루어지는 것으로 간주하고 연속 3 프레임에서 다른 패턴이 검출되면 정보보호 알고리즘 손실을 선언한다. 이 경보를 OHA 에 보고한다. 그리고 이를 송신단에 통보함으로서 정보보호 알고리즘의 동기를 다시 설정한다. F2 채널은 OHA 에 의해 처리되며, OHA 내에 별도의 프로세스를 두어 처리한다.

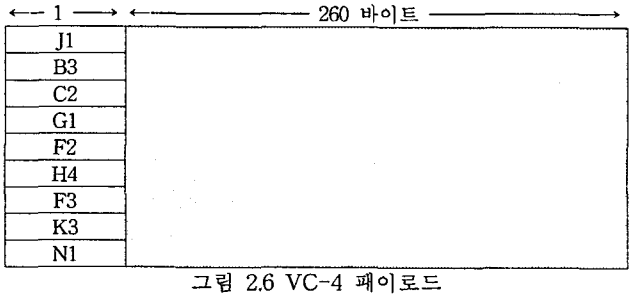

그림 2.6 VC-4 페이로드

정보보호 시스템의 LPT 의 송신부에서는 분배된 키에 의한 페이로드에 대한 스크램블링 기능과 정보보호 알고리즘의 동기 및 키 분배를 위한 F2, F3 바이트를 처리해야 해야 한다는 점에서 기존의 동기식 다중시스템의 LPT 와 다르다.

송신부의 기능은 스크램블링 기능과 POH 삽입 기능으로 분류될 수 있다. 스크램블링 기능에 대한 구체적인 적용 알고리즘은 DES (Data Encryption Standard) 및 IDEA(International Data Encryption Algorithm) 의 CBC 모드와 선형 복잡도가 우수한 난수 계열 발생기를 이용하여 실현되어야 한다.[11,16,20]

경로 추적 기능을 위한 J1 바이트는 하나의 운용자의 영역내에서 인터페이스되는 경우, Higher Order Path Access Point Identifier 로서, 한 바이트의 특정 패턴을 이용하거나, ITU G.831 권고안의 3절에 정의된 SAPI 를 이용한다. 서로 다른 운용자 간에 인터페이스 되는 경우, ITU G.831 권고안의 3절에 정의된 SAPI 을 이용해야 한다. 16-바이트 프레임은 Section Access Point Identifiers 전송 용으로 할당되며, 첫 바이트는 프레임 시작 표시자(Frame Start Marker) 와 이전 프레임의 CRC-7 결과값을 포함하며, 나머지 15 바이트는 ITU-T 권고안 T.50 의 15 개의 문자로 구성된다.

B3 바이트는 오류 감시용 바이트로서, 우수 페리티를 이용한 BIP-8 을 사용한다. 이전에 모든 VC3/4 에 대해 계산하여 현재의 B3 위치에 삽입한다.

C2 바이트는 VC3/4 의 구성을 나타내는 바이트로서, 표 2.1과 같은 상태를 전달한다.

VC3/4 신호를 위한 LPT 의 수신부에서는 POH 추출부와 디스크램블링 부, 그리고 기밀성 알고

리즘 동기 손실 검출부로 구성된다. 추출된 F2, F3 바이트는 OHA 로 전달되며, BIP-8 부호로 부호화된 B3 바이트를 이용하여 패리티 법칙에 어긋난 비트 수를 추출하여 송신단의 REI 계산을 위해 전송하고 또한 S6 인터페이스를 통하여 SEMF 에 전달한다.

G1 바이트의 첫 4 비트는 원격국에서 검출된 BIP-8 부호에서 패리티 법칙이 어긋난 부호의 갯수를 나타내는 REI 부이며, 다섯 번째 비트는 원격단의 FERF(Far End Receive Failure) 상태를 나타낸다. 수신된 C2 바이트를 검사하여 자신의 신호 구성 값과 다를 경우, HP-SLM (HP Signal Label Mismatch) 결함을, 수신된 C2 바이트가 "00000000" 인 경우 UNEQ 결함 상태를 S6 인터페이스를 통해서 SEMF 로 전달한다. J1 바이트를 검사하여 자신이 가지고 있는 정보와 일치하지 않으면 HP-TIM (HP Trace Identifier Mismatch) 상태를 S6 인터페이스를 통해 SEMF 로 전달한다. HP-TIM, HP-SLM, UNEQ 상태가 발령되면 LPT 는 디스크램블링 기능을 중단하고 LPA 로 "all 1" 신호를 전달한다.

표 2.1 C2 바이트 사상 부호

MSB 1 2 3 4	LSB 5 6 7 8	해석
0 0 0 0	0 0 0 0	Unequipped
0 0 0 0	0 0 0 1	Equipped - Non Specific
0 0 0 0	0 0 1 0	TUG 구조
0 0 0 0	0 0 1 1	Locked TU
0 0 0 0	0 1 0 0	북미 및 유럽 방식 비동기식 DS3 신호의 C3 사상
0 0 0 1	0 0 1 0	비동기식 139.264Mbps 신호의 C4 사상
0 0 0 1	0 0 1 1	ATM 사상
0 0 0 1	0 1 0 0	MAN(DQDB) 사상
0 0 0 1	0 1 0 1	FDDI 사상
1 1 1 1	1 1 1 0	O.181 시험 신호
1 1 1 1	1 1 1 1	VC-AIS

위의 사항을 고려한 LPT 및 HPT 의 송신부의 기능 블럭도는 그림 2.7과 같고, 수신부의 기능 블럭도는 그림 2.8과 같다.

나. OHA

기존의 동기식 다중시스템에서의 OHA 에서는 중계 구간 및 다중 구간의 타합선을 위한 E1/E2 바이트의 정보 생성원 및 종단원의 기능을 수행하고 있다. 동기식 정보보호 시스템에서의 OHA 는 이 기능 외에 각 LPT 또는 HPT 에서 송수신되는 F2 바이트 처리 기능이 존재해야 한다.

F2 바이트는 상대 단국과의 키 분배 및 인증 기능을 수행해야 한다. 따라서 이를 위한 별도의 정보 처리 기능이 존재해야 한다. 키 분배 및 인증은 두 시스템간에 여러 개의 VC3/4 신호에 대한 기밀성 서비스가 제공되더라도 이중 하나의 데이타 링크 계층을 이용하여 실현한다. 따라서 OHA 내의 정보처리 기능은 하나 이상의 VC3/4 을 위한 키 분배 기능을 수행해야 한다.

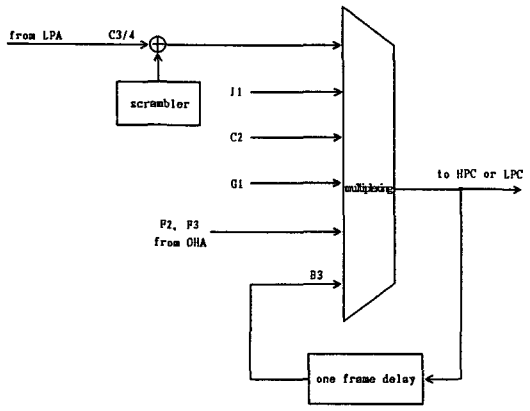

그림 2.7 LPT 및 HPT 송신부의 기능 블럭도

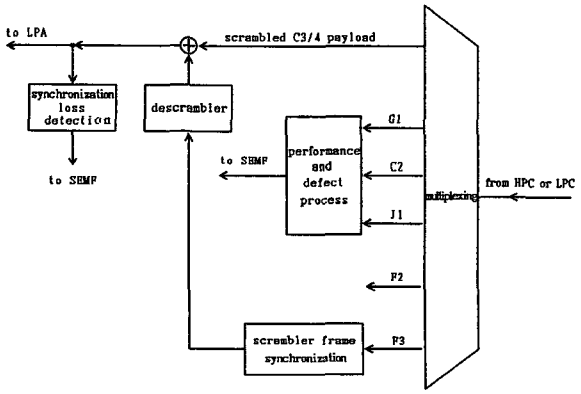

그림 2.8 LPT 및 HPT 수신부의 기능 블럭도

2.6 동기식 전송망에 적용 가능한 키 분배 방식

본 절에서는 동기식 정보보호 시스템에 적용 가능한 4 가지 키 분배 방식을 분석한다. [13]

가. DH 방식의 ElGamal 의 변형

본 방식은 일회 전송으로 개체 A 와 B 간의 공유키를 설정할 수 있다. 준비해야 할 파라메타는 큰 소수 p 와 GF(p) 에서의 원시원 g 이다. 그리고 각 개체는 자신의 고유의 공개키 ($y_X = g^{h_X}$) 와 관용키(h_X) 를 소지하고 있다. 그리고 각 개체는 상대방의 공유키 분배용 공개키에 대한 공인된 복사본을 구할 수 있다. 키 분배 방법은 다음과 같다.

① 개체 A 는 임의의 난수 $r_A \in \{1, \cdots, p-2\}$ 를 선택한 후, $C_A \equiv g^{r_A} \bmod p$ 를 계산하여 C_A 를 개체 B 에 전달한다.

② 개체 A 는 r_A, y_B 를 이용하여 식 (2.1) 과 같은 공유키 K_{AB} 를 계산한다.

$$K_{AB} \equiv (y_B)^{r_A} \equiv g^{r_A h_B} \tag{2.1}$$

③ 개체 B 는 h_B, C_A 를 이용하여 공유키 K_{AB} 를 계산한다.

$$K_{AB} \equiv (C_A)^{h_B} \equiv g^{h_B r_A} \tag{2.2}$$

이 방식은 상대방의 공유키 분배용 공개키를 알고 있다는 가정하에서 일회 전송이 요구되며, 개체 B 에 대한 내재적인 키 인증 기능이 있다. 즉, 개체 B 이외에 어떤 다른 개체도 공유키를 계산할 수 없다. 그러나 이 방식은 키 확신 특성이 없다.

나. Nyberg-Rueppel 방식

본 방식은 상대방의 인증된 공개키를 알고 있다는 가정하에서 일회 전송으로 동작된다. 본 방식은 수신자 B 에 대한 인증 기능이 있으며, 타임 스템프나 일련 번호를 개입하면 엔터티 인증 기능이 제공된다. p 를 큰 소수라고 하고, q 는 p-1 또는 p-1 의 큰 약수이다. g 는 차수가 q 인 GF(p) 상의 원소이다. 그리고 각 개체는 자신의 고유의 공개키($k_X = g^{-s_X}$) 와 관용키 (s_X) 를 소지하고 있다. 각 개체는 상대방의 공유키 분배용 공개키에 대한 공인된 복사본을 구할 수 있다. 키 분배 방법은 다음과 같다.

① 개체 A 는 두개의 임의의 난수 r, $R \in Z_q$ 를 선택한 후 식 (2.3) 을 계산한다. 그리고 개체 B 로 (e, y) 를 전송한다.

$$\begin{aligned} e &= g^{R-r} \bmod p \\ y &= r + s_A e \bmod q \end{aligned} \tag{2.3}$$

② 개체 A 는 다음과 같이 공유키 K_{AB} 를 계산한다.

$$K_{AB} = (k_B)^R = g^{-Rs_B} \tag{2.4}$$

③ (e, y) 를 수신한 개체 B 는 식 (2.5) 와 같이 공유키 K_{AB} 를 계산한다.

$$K_{AB} = (g^y k_A{}^e e)^{s_B} \bmod p = g^{-Rs_B} \tag{2.5}$$

본 방식은 쌍방에서 내재적인 키 인증 기능이 있으나 키 확인 기능이 없다. 만약 해쉬함수 값이 개체 B 로 향하는 데이타에 포함되면 단방향 키 확인 기능이 제공된다. 타임 스탬프나 일련 번호가 개입되면 개체 A 의 개체 B 에 대한 엔터티 인증 기능이 제공된다. 개체 A 는 자신이 난수를 선택하므로 공유키의 키 신선성을 보장받을 수 있으나 개체 B 는 보장받을 수 없다. 일련 번호와 타임스탬프와 함께 키 토큰에 대한 서명 시스템을 사용함으로서 재생공격을 방지할 수 있다.

다. ISO 9798-3 에서의 키 공유 방식

본 방식에서는 Diffie-Hellman 의 기본 파라메타를 가정하고 비대칭형 서명 및 검증 알고리즘의 공개키 및 관용키인 (S_X, V_X) 이 주어졌다고 가정한다. 키 분배는 다음과 같은 프로토콜로 실행된다.

① 개체 A 는 임의의 난수 $r_A \in \{1,\cdots,p-2\}$ 를 선택한 후 g^{r_A}을 계산하여 식 (2.6) 과 같은 토큰을 생성한다. 그리고 개체 B 로 키 토큰을 전송한다.

$$KT_{A1} = g^{r_A} \mod p \tag{2.6}$$

② 개체 B 는 임의의 난수 $r_B \in \{1,\cdots,p-2\}$ 를 선택한 후 g^{r_B} 을 계산하고 식 (2.7) 과 같은 토큰을 생성한다. 그리고 개체 A 로 키 토큰을 전송한다.

$$KT_{B1} = S_B(g^{r_B} \| g^{r_A} \| ID_A) \tag{2.7}$$

③ KT_{B1} 를 수신한 개체 A 는 개체 B 의 서명문을 검증하고 자신이 송신한 g^{r_A} 와 서명문으로부터 획득한 g^{r_A} 이 동일한가를 검사한다. 만약 동일하면 식 (2.8) 과 같이 공유키 K_{AB} 를 계산한다.

$$K_{AB} = (g^{r_B})^{r_A} = g^{r_A r_B} \tag{2.8}$$

그리고 식 (2.9) 와 같은 서명문 키 토큰을 생성하여 개체 B 에 전송한다.

$$KT_{A2} = S_A(g^{r_A} \| g^{r_B} \| ID_B) \tag{2.9}$$

④ KT_{A2} 를 수신한 개체 B 는 개체 A 의 서명문을 검증하고 자신이 송신한 g^{r_B} 와 서명문으로부터 획득한 g^{r_B} 이 동일한가를 검사한다. 만약 동일하면 식 (2.10) 과 같이 공유키 K_{AB} 를 계산한다.

$$K_{AB} = (g^{r_B})^{r_A} = g^{r_A r_B} \tag{2.10}$$

본 방식은 상호 개체 인증 기능을 갖지만 키 확신 특성은 제공하지 않는다. 본 방식은 DH 의 키

분배 메카니즘과 서명 메카니즘이 요구되며 삼회 전송으로 완료된다. 각 개체는 자신이 선택한 난수가 공유된 키의 파라메타로 기여하므로 공유된 키에 대한 신선도를 보장받는다. 키 토큰들 KT_{B1}, KT_{A2} 에 공유키 K_{AB} 의 해쉬값을 부가함으로서 쌍방 키 확신 기능을 제공할 수 있다.

라. 자가 입증(self-certifying) 공개키에 의한 키 공유 기법

본 절에서는 Girault 가 제시한 자가 입증 공개키에 기초한 키 공유 프로토콜을 분석한다.[17] 정수 n 은 RSA 정수이고 원소 g 는 Z_n 에서 최대의 차수를 갖는 원소이며, T 는 믿을 수 있는 센타로서 n 의 소인수들을 알고 있고, 따라서 RSA 공개키와 관용키 쌍을 알고 있다. 개체 A 는 자신의 관용키 s_A 를 선택하고, 자신의 공개키 $g^{-s_A} \mod n$ 를 계산하여 공개키 센타에 전달한다. 그리고 개체의 이름과 주소로 구성되는 I_A 를 구성한다. T 는 식 (2.11) 과 같은 개체 A 의 공개키 증명서 역할을 수행하는 사용자 A 의 공개키를 계산한다.

$$P_A = (g^{-s_A} - ID_A)^d \mod n \tag{2.11}$$

식 (2.11) 로 부터 식 (2.12) 을 알 수 있다.

$$P_A^e + ID_a = g^{-s_A} \mod n \tag{2.12}$$

개체 B 도 동일한 방법으로 개체 B 의 공개키 증명서를 구할 수 있다. 임의의 개체는 모든 개체의 공개키 증명서로부터 개체의 공개키를 구할 수 있다. 키 공유 방식은 다음과 같이 세 가지이다.

(P1) 데이타 토큰의 교환없이 개체 A,B 는 식 (2.13) 을 이용하여 공유키를 구할 수 있다.

$$\begin{aligned} K_{AB} &= (P_A^e + ID_A)^{s_B} \\ &= (P_B^e + ID_B)^{s_A} \\ &= g^{-s_A s_B} \mod n \end{aligned} \tag{2.13}$$

(P2) 이 프로토콜은 일회 전송으로 수행되며 개체 A, B 는 식 (2.14) 와 식 (2.15) 와 같은 공유키를 구할 수 있다.

① 개체 A 는 임의의 난수 r_A 를 선택하고 g^{r_A} 를 개체 B 로 전송한다. 개체 A 는 식 (2.14) 와 같이 공유키를 계산한다.

$$\begin{aligned} K_{AB} &= (P_B^e + ID_B)^{-r_A} \\ &= g^{-r_A s_B} \mod n \end{aligned} \tag{2.14}$$

② g^{r_A} 를 수신한 개체 B 는 식 (2.15) 와 같이 공유키를 계산한다.

$$K_{AB} = (g^{s_A} g^{r_A}(P_A^e + ID_A))^{s_B} = g^{-r_A s_B} \mod n \quad (2.15)$$

(P3) 이 프로토콜은 이 회 전송으로 수행되며 개체 A,B 는 다음과 같은 공유키를 구할 수 있다.

① 개체 A 는 임의의 난수 r_A 를 선택하고 g^{-r_A} 를 개체 B 로 전송한다.

② 개체 B 는 임의의 난수 r_B 를 선택하고 g^{-r_B} 를 개체 A 로 전송한다.

③ g^{-r_B} 를 수신한 개체 A 는 식 (2.16) 과 같이 공유키를 계산한다.

$$K_{AB} = (g^{-r_B})^{s_A}(P_B^e + ID_B)^{r_A} = g^{-s_B r_A - s_A r_B} \mod n \quad (2.16)$$

④ g^{-r_A} 를 수신한 개체 B 는 식 (2.17) 과 같이 공유키를 계산한다.

$$K_{AB} = (g^{-r_A})^{s_B}(P_A^e + ID_A)^{r_B} = g^{-s_B r_A - s_A r_B} \mod n \quad (2.17)$$

P1 은 쌍방 키 인증 기능을 제공하며, P2 는 일방향 내재적인 키 인증 기능을 제공하며, P3 는 쌍방향 내재적인 키 인증 기능을 제공한다. 세 프로토콜은 키 확신 기능이 없으며 재생 공격에 대한 대비책도 없다.

2.7 공개키 증명서의 실현

본 절에서는 동기식 정보보호 시스템에 적용될 수 있는 공개키 증명서의 구조를 제시하고, 이를 MD5 해쉬 함수와 RSA 기밀성 알고리즘을 이용하여 실현한다.[16]

공개키 증명서의 구성 정보는 사용자의 공개키와 사용자의 구별 가능한 이름, 공개키 증명서의 유효 기간 등이며, 공개키 증명서는 상기 구성 신호를 CA(Certificate Authority) 의 비밀키로 서명한 $D_{CA_S}(ID_A, PK_A)$ 이다. 공개키 증명서의 검증은 CA 의 공개 정보를 이용하여 수행되며, CA 의 공개 정보는 각 사용자가 변경 불가능한 영역에 보관해야 한다. 공개키 증명서의 일반적 구조는 그림 2.9 의 입력 정보와 이에 대한 해쉬 결과 값을 서명한 서명문으로 구성된다.

공개키 증명서의 입력 데이타는 그림 2.9 와 같다.

일련 번호	서명 알고리듬의 종류	발행기관	시작 유효기간	종료 유효기관	이름
000000	01	KIISC (4b4949534 3000000)	1995.10.01. (19951001)	2000.09.03. (20000930)	HYYOUM (4859594f554d00 0000000000)
← 24 →	← 8 →	← 64 →	← 32 →	← 32 →	← 96 →

사용자의 공개키1(e)	사용자의 공개키2(n)	사용자의 공개키 알고리듬의 종류	패딩 부 및 길이
65537 (0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000000000 0000000000010001)	0000c250f39c7325 41e9ceb0869ae9e5 51b7cd5109f03ce1 4a4810b653d4ae3a 5104ca2697b0dc90 b1b9e728697ac7c2 0817f1beab0c028c ea56eba457397a75	00000001	8000000000000000 0000000000000000 0000000000000000 00000520
← 512 →	← 512 →	← 32 →	← 224 →

그림 2.9 공개키 증명서의 입력 데이타

상기 정보를 MD5 해쉬 함수에 적용한 출력 해쉬 값은 식 (2.18) 과 같다.

출력 해쉬 값 = [9d510a3e] [9fb2fb36] [57a79160] [52d50e89] (2.18)

CA 에서 이용되는 RSA 의 공개키중 합성수 n, 서명용 비밀키 d, 그리고 공개키 e 는 식 (2.19) 와 같다.

n = 0000 c250 f39c 7325 41e9 ceb0 869a e9e5 51b7 cd51 09f0 3ce1 4a48 10b6
53d4 ae3a 5104 ca26 97b0 dc90 b1b9 e728 697a c7c2 0817 f1be ab0c 028c
ea56 eba4 5739 7a75

d = 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 014d

e = 0000 66b3 a046 634b cfcf 5ea2 7cf4 daf2 aace 4f4d 6d09 59d5 a17e 7f39
2876 8ed2 b49b 681b 931b bbb4 7814 8c65 3f62 f261 ef5f 2ff8 b762 80c6
d885 a055 db52 c8c5 (2.19)

해쉬 결과 값을 식 (2.19) 와 같은 RSA 알고리즘에 적용하면 그림 2.10 과 같은 서명문을 구할 수 있다.

$D_S(H(I))$

0000 87b2 bbb8 d08a 780a e9d6 d578 74e4 cda7 3c6a 4770 25f2 3f29 7ec0 d223 2045
d78a 4027 7eb1 bf73 859a 0f15 0fa6 79c5 4806 a83c 528f 8fd8 c7fd 5640 a582 3ee4
← 512 비트 →

그림 2.10 해쉬 결과

각 사용자의 공개키 증명서는 그림 2.9와 같은 정보와 그림 2.10과 같은 해쉬 결과 값을 쇄상한 값이 된다. 이는 C 언어로 구현되었으며, RSA 의 키 생성을 위한 안전성에 대한 요구 조건을 모

두 만족하도록 실현되었다. 시뮬레이션 결과 공개키 증명서가 정상적으로 동작됨을 확인하였다.

3. 결 론

동기식 다중시스템에 정보보호 기능을 부가한 동기식 정보보호 시스템은 동기식 전송망이 확대됨에 따라 기간 전송망의 정보보호 시스템으로 널리 활용될 예정이다. 동기식 정보보호 시스템은 근본적으로 동기식 다중시스템이므로 ITU G 시리즈 권고안을 따라서 설계되어야 한다.

본 고에서는 기존의 SDH 시스템의 주요 기능 및 특성을 제시하였고, 이를 변경한 동기식 정보보호시스템에 적용될 수 있는 인증 방식, 키 분배 방식, 그리고 정보보호방식을 제안하였다. 제시된 정보보호 메니즘은 정보보호 시스템을 위한 모든 요구 사항을 만족하므로 동기식 정보보호 시스템 실현시 유용하게 활용될 수 있음을 확인하였다. 그리고 제안된 구조는 기존의 동기식 다중시스템과 호환성이 있게 연동될 수 있고 기존의 동기식 다중시스템에 최소로 변경하여 실현될 수 있음을 확인하였다. 그리고 RSA 와 MD5 알고리즘을 이용한 공개키 증명서를 C 언어를 이용하여 실현하였고, 관련 기능을 시뮬레이션하였다. 시뮬레이션 결과 정상적으로 동작될 수 있음을 확인할 수 있었다. 본 연구의 결과는 동기식 정보보호시스템의 실현시에 적극적으로 활용될 수 있다.

- 참 고 문 헌 -

(1) ITU-T Rec. G.707, Synchronous Digital Hierarchy Bit Rate, 1988.

(2) ITU-T Rec. G.708, Network Node Interface for the Synchronous Digital Hierarchy, 1988.

(3) ITU-T Rec. G.709, Synchronous Multiplexing Structure, 1988.

(4) TR-TSY-000253, Synchronous Optical Network Transport Systems: Common Generic Criteria, Bellcore, 1989.

(5) ITU-T Rec. G.782, Type and General Characteristics of Synchronous Digital Hierarchy Equipment, 1994.

(6) ITU-T Rec. G.783, Characteristics of Synchronous Digital Hierarchy Equipment Functional Blocks, 1994.

(7) ITU-T Rec. G.784, Synchronous Digital Hierarchy Management, 1994.

(8) ISO/IEC 9798-1, Information Technology - Entity Authentication Mechanism, Part 1; General Model, ISO, Geneva, Switzerland, 1993.

(9) ISO/IEC 9798-2, Information Technology - Entity Authentication Mechanism, Part 2; Mechanisms Using Symmetric Encipherment Algorithms, ISO, Geneva, Switzerland, 1993.

(10) ISO/IEC IS 9798-3, Entity Authentication Mechanisms - part 3 : Entity Authentication Using a Public-key Algorithm, ISO, Geneva, Switzerland, 1993.

(11) M.Y. Rhee, Cryptography and Secure Communications, McGraw-Hill, 1993.

(12) S.Tsujii and M.O. Kasahara, Cryptography and Information Security, 昭晃堂, 1990.

(13) R.A. Rueppel and P.C.V. Oorschot, "Modern Key Agreement Techniques," Computer Communications, Vol.17, No.7, pp.458-465, 1994.

(14) T.ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Inform. Theory, Vol.31, pp.467-472, 1985.

(16) G.J.Simmon, Contemporary Cryptology, IEEE press, 1992.

(17) M.Girault, "Self-certificated Public Keys," Eurocryt'91, Springer-Verlag, pp.480-487, 1991.

(18) ISO/IEC CD 11770-3, Key Management - part 3 ; Key Management Mechanisms using Asymmetric Techniques, ISO, Geneva, Switzerland, 1993.

(19) ITU Rec. X.509, The Directory - Authentication Framework, ITU, Geneva, Switzerland, 1993.

(20) HeungYoul Youm and ManYoung Rhee, "Correlation-immune Random Sequence Generator Using GMW Sequences," Proceeding of Joint Workshop on Information Security and Cryptography'95, Japan, 1995.