TTA Standard

정보통신단체표준(국문표준) 제정일: 200x 년 xx 월 xx 일

TTAx.xx-xx.xxxx

디지털 협대역 무전기의 (12.5kHz, TDMA) 암호화

DMR Encryption

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회		공공안전통신 프로젝트그룹(PG902)			
표준안 심의 위원회		전파/이동통신 기술위원회(TC9)			
	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	천인욱	유니모테크놀로지	수석연구원	위원	
표준 초안 작성자	홍영삼	모토로라솔루션	상무	의장	
	김응배	한국전자통신연구원I	책임연구원	부의장	
	김동찬	한국네트워크산업협회	전문위원	부의장	
	천인옥	유니모테크놀로지	수석연구원	위원	
	황철구	모토로라솔루션	부장	위원	
	김대윤	하이테라커뮤니케이션	이사	-	
	Thomas Bohn	모토로라솔루션	부장	-	
사무국 담당	김대중	TTA	단장		
	장민욱	TTA	책임		

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 표준의 목적

이 표준의 목적은 DMR 디지털 협대역 무전기(12.5kHz, TDMA)의 암호화에 대하여 정의함으로서 모든 DMR 디지털 협대역 무전기 간의 암호화 모드에서의 호환성을 보장하기 위함이다.

2 주요 내용 요약

이 표준은 DMR 디지털 협대역 무전기(12.5 KHz TDMA)의 암호화를 위한 여러 단계별 음성처리 과정 중에서 음성처리 단계를 정의하며 이러한 정의된 단계에서 음성 데이터 배열 방안에 대하여 표준화를 한다.

3 인용 표준과의 비교

해당 사항 없음

3.1 인용 표준과의 관련성

DMR 협회의 DMR Encryption, ARC4 Encryption for DMR Association, 'DMR CAI Transmit Bit Order with AMBE_2 Vocoder'와 ETSI TS 102 361-1 DMR Air Interface 을 그대로 인용함.

3.2 인용 표준과 본 표준의 비교표

본 표준	인용 표준	비고
5 DMR 암호화	DMR 협회의 DMR Encryption과 ARC4 Encryption for DMR Association	**동일** **단, AES256 만 선택함**
6. 음성 암호화		
일반	**ETSI TS 102 361-1 5.1.2.1 절과 6.2 절**	**동일**
음성 통화 후발 진입을 지원하는 키 ID 와 알고리즘 ID 시그널링	**ETSI TS 102 361-1 6.1 절, 9.1.2 절, 9.3.2 절 및 9.3.3 절**	**동일**

비 역방향 채널 단일 버스트 BPTC	**ETSI TS 102 361-1 B.2.2.1 절**	동일
음성 통화의 후발 진입을 지원하는 IV 시그널링	**DMR 협회의 'DMR CAI Transmit Bit Order with AMBE_2 Vocoder' ETSI TS 102 361-1, 5.1.2.1 절과 6.1 절**	동일
7. 데이터 암호화	**ETSI TS 102 361-1 5.1.3.1 절과 8.2.1.4 절**	동일

Preface

1 Purpose

The standard is for defining encryption of DMR radio

2 Summary

Encryption for voice and data of DMR radio is defined based upon

- DMR Encryption for DMR Association
- ARC4 Encryption for DMR Association
- ETSI TS 102 361-1 cl. 5.1.2.1, 5.1.3.1, 6.2, 8.2.1.4, 9.3.2, and B.2.2.1

3 Comparison with Reference Standards

3.1 Relationship to Reference Standards

The following reference standards are referred without any change

- DMR Encryption for DMR Association
- ARC4 Encryption for DMR Association
- ETSI TS 102 361-1 cl. 5.1.2.1, 5.1.3.1, 6.2, 8.2.1.4, 9.3.2 and B.2.2.1

3.2 Comparison of this standard with Reference Standards

This Standard	**Reference Standards**	**Remark**
5 DMR Encryption	DMR Association: DMR Encryption, and ARC4 Encryption for DMR Association	**Identical** **But, AES256 only selected**
6. Voice Encryption		
General	**ETSI TS 102 361-1, cl. 5.1.2.1 and 6.2**	**Identical**
Key ID and Algorithm ID signaling to support voice late entry	**ETSI TS 102 361-1, cl. 6.2, 9.1.2, 9.3.2 and 9.3.3**	**Identical**
Non-Reverse Channel Single Burst BPTC	**ETSI TS 102 361-1, cl. B.2.2.1**	**Identical**
IV signaling to support voice late entry	**'DMR CAI Transmit Bit Order with AMBE_2 Vocoder' of DMR Association**	**Identical**

	ETSI TS 102 361-1, cl. 6.1 and 5.1.2.1	
7. Data Encryption	**ETSI TS 102 361-1, cl. 5.1.3.1 and 8.2.1.4**	**Identical**

목 차

디지털 협대역 무전기의 (12.5kHz, TDMA)

암호화

(DMR Encryption)

1 적용 범위

본 표준은 디지털 협대역 무전기(12.5kHz, TDMA)의 상호 호환성 확보를 위하여 암호화(Encryption) 처리 전에 음성 데이터 단계와 배열에 대하여 기술하며 TTAE.ET-TS 102 361-1의 표준이 적용되는 디지털 협대역 무전기(12.5kHz, TDMA)를 이용하여 음성 및 데이터 서비스를 제공하는 1GHz 주파수 범위 이하에서 사용되는 디지털 무전기에 적용한다.

2 인용 표준

- DMR Encryption
- ARC4 Encryption for DMR Association
- ETSI TS 102 361-1 5.1.2.1 절, 5.1.3.1 절, 6.2 절, 9.3.2 절, 8.2.1.4 절, B.2.2.1 절

3 용어 정의

- 해당 없음

4 약어

AES	Advanced Encryption Standard
BPTC	Block Product Turbo Code
CBSK	Control Signalling BlocK
DES	Data Encryption Standard
DPF	Data Packet Format
DMR	Digital Mobile Radio
FEC	Forward Error Correction
IV	Initialization Vector
LC	Link Control

MBC	Multiple Block Control packets
MFID	Manufacturer's FID
PC	Parity Check bit
PI	Privacy Indicator
SAP	Service Access Point
SB	SimBol
Sync	Syncronization

5 DMR 암호화

본 표준에서의 DMR 암호화는 DMR 협회가 정의하는 DMR 암호화와 AES256 를 사용한다.

그리고 DMR 암호화는 음성과 데이터의 암호화를 모두 다루며 자세한 내용은 다음의 두건의 문서에 기술되어 있다:

- DMR Encryption
- ARC4 Encryption for DMR Association

첫번째 문서는 AES256 암호화 알고리즘을 두번째 문서에서는 암호화 파라미터들이 무선 구간에 걸쳐 어떻게 전송되는지를 자세히 기술한다. 음성 솔루션이 AMBE+2 보코더와 복잡하게 연계되어 있기 때문에, 'DMR CAI Transmit Bit Order with AMBE+2 vocoder' 또한 참조하여야 한다.

음성 및 데이터 암호화 방법은 두 건의 표준, 즉 DMR 암호화 및 DMR 협회의 ARC4 암호화에 자세히 기술되어 있다. 이 문서들을 획득하려면 제조업체는 DMR 협회의 회원이 되어야 한다. TTA 는 암호화 솔루션으로 ETSI DMR/DMR 협회 암호화 솔루션을 이용할 것이 제안된다. 다음의 기술적 개요는 이 솔루션을 설명한다.

Over the Air 시그널링 파라미터

The encryption parameters sent over the air are:

- 알고리즘 ID (3 비트, 4 개가 정의됨)
- 키 ID (8 비트, 255 개 지원됨)
- 초기화 백터 (32 비트)

이 파라미터들이 어떻게 무선구간에 걸쳐 전송되는 것은 음성과 데이터가 상이하다. 음성과 데이터 솔루션의 자세한 부분을 아래에 기술한다. DMR 협회의 암호화 솔루션에 현재 정의된 암호화 알고리즘은 다음과 같이 4가지가 있으나 본 표준에서는 AES256만을 선택한다.

- ARC4 (40 bit key)
- DES (64 bit key)
- AES128 (128 bit key)
- AES256 (256 bit key)

DMR 협회 솔루션에서와 같이 하나 이상의 알고리즘이 지원될 때 특정 암호화 알고리즘을 명시적으로 확인해주는 알고리즘을 송신한다.

키 ID는 사전 프로그래밍된 키를 나타내기 위해 구성된다. 실제 키는 무선으로 전송되지

않고 사전 프로그래밍된 식별자를 통해서만 전송된다. 이 구현에서는 최대 255개의 키가 지원된다.

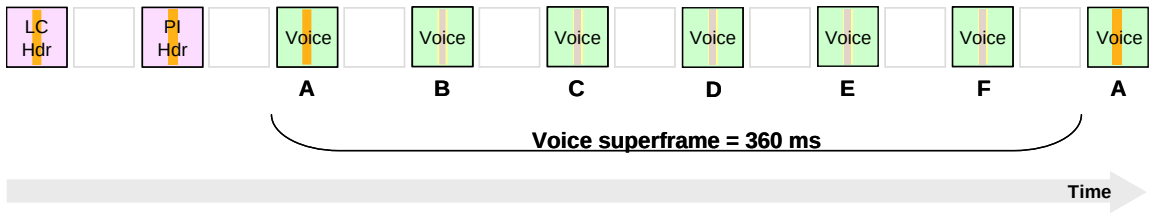
초기화 벡터(IV)는 동일한 평문 메시지를 여러 번 암호화하면 암호화된 메시지가 매번 서로 달라지는 랜덤마이저 역할을 하므로 중요하다. 따라서 데이터 반복이 방지되고 해커가 패턴을 찾기 어려워지므로 궁극적으로 알고리즘을 파괴하기 어려워진다.

6. 음성 암호화

<출처: ETSI TS 102 361-1 5.1.2.1절과 6.2절>

ETSI TS 102 361-1은 무선 암호화 시그널링을 지원하기 위한 기반이 된다. 이는 프라이버시 지시자(PI) 헤더를 식별하는 (그림 6-1)과 <표 6-1>에 설명되어 있다.

컨벤셔널 시스템의 경우, (그림 6-1)에 설명된 것처럼 음성 LC 헤더가 전송되고 PI 헤더는 음성 전송이 시작될 때 전송될 수 있다. 이 경우, 음성 LC 헤더는 PI 헤더 앞에 와야 한다.



(그림 6-1) LC와 PI 헤더를 포함한 음성 전송 개시

<표 6-1> 데이터 유형 정보 요소 정의

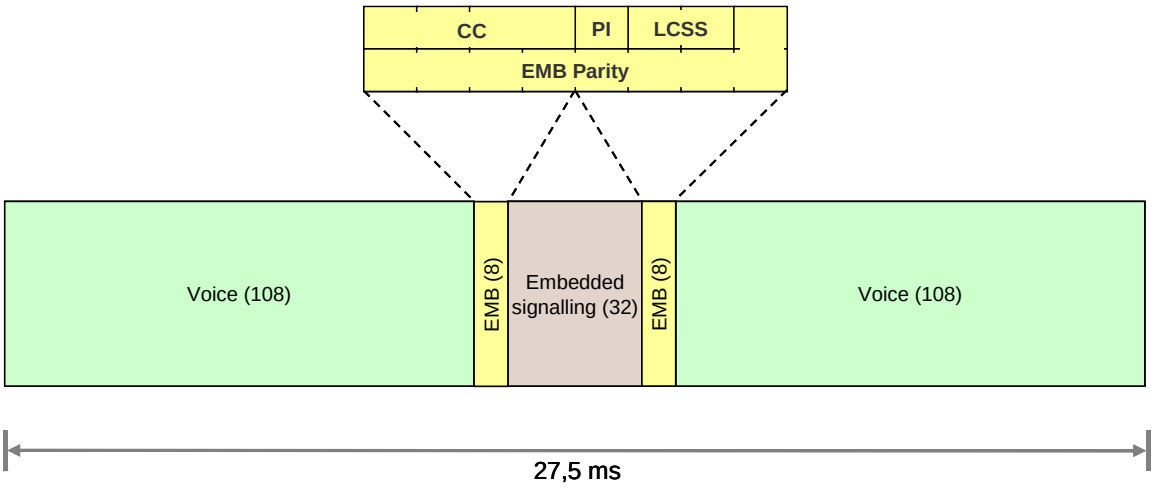
데이터 유형	목적	페이로드 FEC
PI 헤더, 주 참조	독립형 버스트의 프라이버시 지시자 정보	BPTC(196,96)
음성 LC 헤더	음성 전송의 시작을 나타내며 주소 지정 정보를 전달한다.	BPTC(196,96)
LC 포함 종료자	음성 전송의 종료를 나타내며 LC 정보를 전달한다.	BPTC(196,96)
CSBK	제어 블록을 전달한다.	BPTC(196,96)
MBC 헤더	다중 블록 제어용 헤더	BPTC(196,96)
MBC 연속화	다중 블록 제어용 계승 블록	BPTC(196,96)
데이터 헤더	패킷 데이터 블록의 주소 지정 및 번호 전달	BPTC(196,96)
$\frac{1}{2}$ 데이터 연속	$\frac{1}{2}$ 속도 패킷 데이터용 페이로드	BPTC(196,96)
$\frac{3}{4}$ 데이터 연속	$\frac{3}{4}$ 속도 패킷 데이터용 페이로드	Rate $\frac{3}{4}$ Trellis
유휴	전송할 정보가 없을 때 채널을 채운다.	BPTC(196,96)
통합 단일 블록 데이터	단일 블록에서 제어 및/또는 데이터 페이로드를 전송한다.	BPTC(196,96)
주: 이 정보 요소는 본 문서에서 정의되지 않으며 추후 사용을 위해 예약된다		

<표 6-1>의 주(NOTE)는 프라이버시 헤더가 ETSI DMR에는 정의되어 있지 않지만 DMR 협회의 두 건의 문서에서 정의되어 있다. 이는 (그림 6-2)에서와 같이 음성 페이로드 이전에 암호화 정보(키 ID, 알고리즘 ID 및 IV)를 전송할 수 있도록 한다 .

평문 음성 전송에서, 음성 헤더를 누락시키면 통화로 후발 진입이 가능하다. 이는 음성 헤더 정보를 음성 버스트 B－E의 임베디드 신호로 전달함으로써 지원된다. 후발 진입 기능은 DMR 협회 솔루션에 의하여 암호화된 음성 통화에도 지원된다. 이에는 두 개의 방법이 있다. 하나는 Key ID와 알고리즘 ID을, 다른 방법은 IV를 전송하는 방법이다.

음성 통화 후발 진입을 지원하는 키 ID와 알고리즘 ID 시그널링

키 ID와 알고리즘 ID 정보를 보내기 위해 음성 버스트 F에서 임베디드 시그널링이 이용된다. (그림 6-2) (ETSI TS 102 361-1 6.1절)은 임베디드 시그널링을 갖는 음성 버스트를 나타낸다.



(그림 6-2) 임베디스 시그널링을 갖는 음성 버스트

EMB 필드는 ETSI TS 102 361-1 9.1.2절에 더 자세히 정의 되어 있다. 암호화 파라메터와 하나의 CRC가 비 역방향 채널 임베디스 시그널링에 의해 하나의 버스트로 전송되기 때문에, ETSI TS 102 361-1 9.3.2절과 9.3.3절에서와 같이 EMB 필드에서 PI 비트와 LCSS 비트들은 0_2과 00_2으로 각각 설정된다. 이는 <표 6-2> (ETSI TS 102 361-1 표1) 및 <표 6-3> (ETSI TS 102 361-1 표2)와 같다.

<표 6-2> 프라이버시 표시자

정보 요소	길이	값	비고
선취와 출력 제어 표시자	1	0_2	임베디드 시그널링이 동일한 논리 채널이나 NULL 임베디드 메시지 (주 참조)와 관련된 정보를 전달 한다. (주 참조)
		1_2	임베디드 시그널링은 다른 논리 채널과 관련된 RC 정보를 전달한다. (주 참조)
주: 이는 정렬된 타이밍 (ETSI TS 102 361-1 5.1.1.1절 참조)을 나타내며; 오프셋 채널 타이밍 (ETSI TS 102 361-1 5.1.1.2절 참조)의 경우는 PI = 0 과 PI = 1 모두가 동일 논리 채널을 나타낸다.			

<표 6-3> LC 시작/종료 (LCSS)

정보 요소	길이	값	비고
LC 시작/종료	2	00_2	하나의 단편 LC 또는 첫 단편 CSBK 시그널링. 주 참조
		01_2	LC 시그널링의 첫 단편
		10_2	LC의 마지막 단편 또는 CSBK 시그널링
		11_2	LC의 연속 단편 또는 CSBK 시그널링
주: CACH 시그널링으로 정의된 LC의 하나의 단편은 없다			

임베디드 시그널링의 32 비트는 키 ID, 알고리즘 ID, CRC 및 FEC로 구성된다.. 더 자

세한 내용은 DMR 협회 문서를 참조한다. <표 6-4>는 일반적 솔루션을 나타낸다.

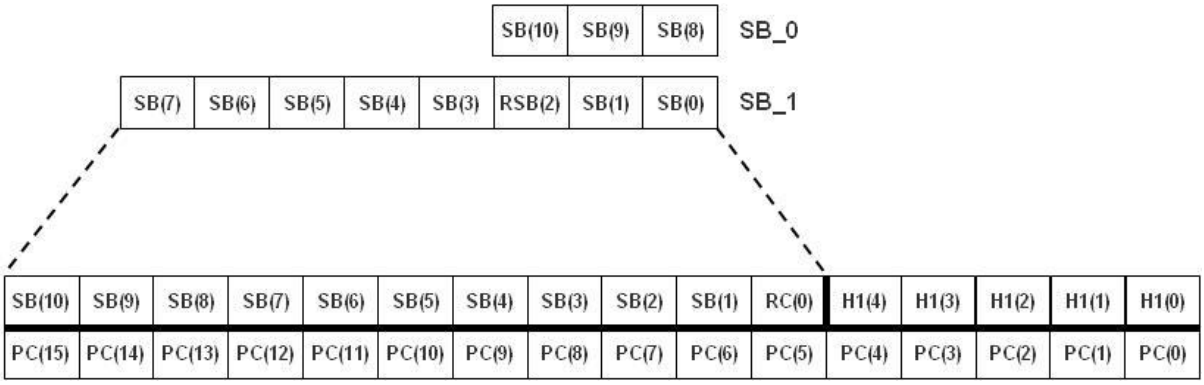
<표 6-4> 음성 암호화 임베디드 시그널링의 예

정보 요소	길이	비고
키 ID	8	
알고리즘 ID	3	
CRC 와 FEC	21	

비 역방향 채널 단일 버스트 BPTC

<출처: ETSI TS 102 361-1 B.2.2.1절>

비 RC 단일 버스트 FEC는 임베디드 신호 코드의 특별한 경우이며, 임베디드된 키 ID와 알고리즘 ID 정보를 전달한다. BPTC 인코더 행렬 형식은 가변 길이 임베디드 신호와 동일하다. 그러나, 인터리빙은 단일 버스트에 대하여 에러에 대한 추가적인 저항을 제공하기 위해 다르게 수행된다. (그림 6-3)은 비 RC 단일 버스트 시그널링에 대한 부호화의 세부사항을 나타낸다. 비 RC 단일 버스트 신호의 11비트인 SB(10) - SB(0)는 행렬의 첫 번째 행에 배치되고 해빙 (16,11,4) 코드로 보호된다. 맨 아래 행에는 각 열에 대한 짝수 패리티 검사 비트가 포함된다. 이 경우, 패리티 검사 행은 정보 행과 동일하다.



(그림 6-3) 비 역방향 채널 단일 버스트 형식

전송을 위해 비트들을 인터리빙하는 첫 번째 단계는 FEC 인코더 행렬 비트에 위에서 아래로, 왼쪽에서 오른쪽으로 순차적으로 번호를 매기는 것이다. <표 5-2>는 해당 색인과 함께 인코더 행렬의 비트를 열거한다. 그런 다음 각 비트는 인터리브 된 배열에서 새 색인에 할당된다. 여기서,

$$\text{Interleave Index} = \text{Index} \times 17 \text{ modulo } 32$$

인터리브 색인의 값은 임베디드 필드에 놓이는 전송 배열의 각 비트의 위치를 결정한다.

<표 6-5> 비 역방향 채널 단일 버스트의 인터리빙 색인

비트	색인	인터리브 색인
SB(10)	0	0
PC(15)	1	17
SB(9)	2	2
PC(14)	3	19
SB(8)	4	4
PC(13)	5	21
SB(7)	6	6
PC(12)	7	23
SB(6)	8	8
PC(11)	9	25
SB(5)	10	10

비트	색인	인터리브 색인
PC(10)	11	27
SB(4)	12	12
PC(9)	13	29
SB(3)	14	14
PC(8)	15	31
SB(2)	16	16
PC(7)	17	1
SB(1)	18	18
PC(6)	19	3
SB(0)	20	20
PC(5)	21	5

비트	색인	인터리브 색인
H(4)	22	22
PC(4)	23	7
H(3)	24	24
PC(3)	25	9
H(2)	26	26
PC(2)	27	11
H(1)	28	28
PC(1)	29	13
H(0)	30	30
PC(0)	31	15

<표 6-6>은 인터리빙 후 비트 정렬을 열거한다. 색인 값 0부터 31은 이전의 표의 인터리브 색인에 해당한다. 결과 배열에는 임베디드 필드에 배치하기 위해 TX(31)부터 TX(0)까지 번호가 매겨진 32비트가 포함된다.

<표 6-6> 비 역방향 채널 단일 버스트의 전송 비트 정렬

색인	비트	TX 비트
0	SB(10)	TX(31)
1	PC(7)	TX(30)
2	SB(9)	TX(29)
3	PC(6)	TX(28)
4	SB(8)	TX(27)
5	PC(5)	TX(26)
6	SB(7)	TX(25)
7	PC(4)	TX(24)
8	SB(6)	TX(23)
9	PC(3)	TX(22)
10	SB(5)	TX(21)

색인	비트	TX 비트
11	PC(2)	TX(20)
12	SB(4)	TX(19)
13	PC(1)	TX(18)
14	SB(3)	TX(17)
15	PC(0)	TX(16)
16	SB(2)	TX(15)
17	PC(15)	TX(14)
18	SB(1)	TX(13)
19	PC(14)	TX(12)
20	SB(0)	TX(11)
21	PC(13)	TX(10)

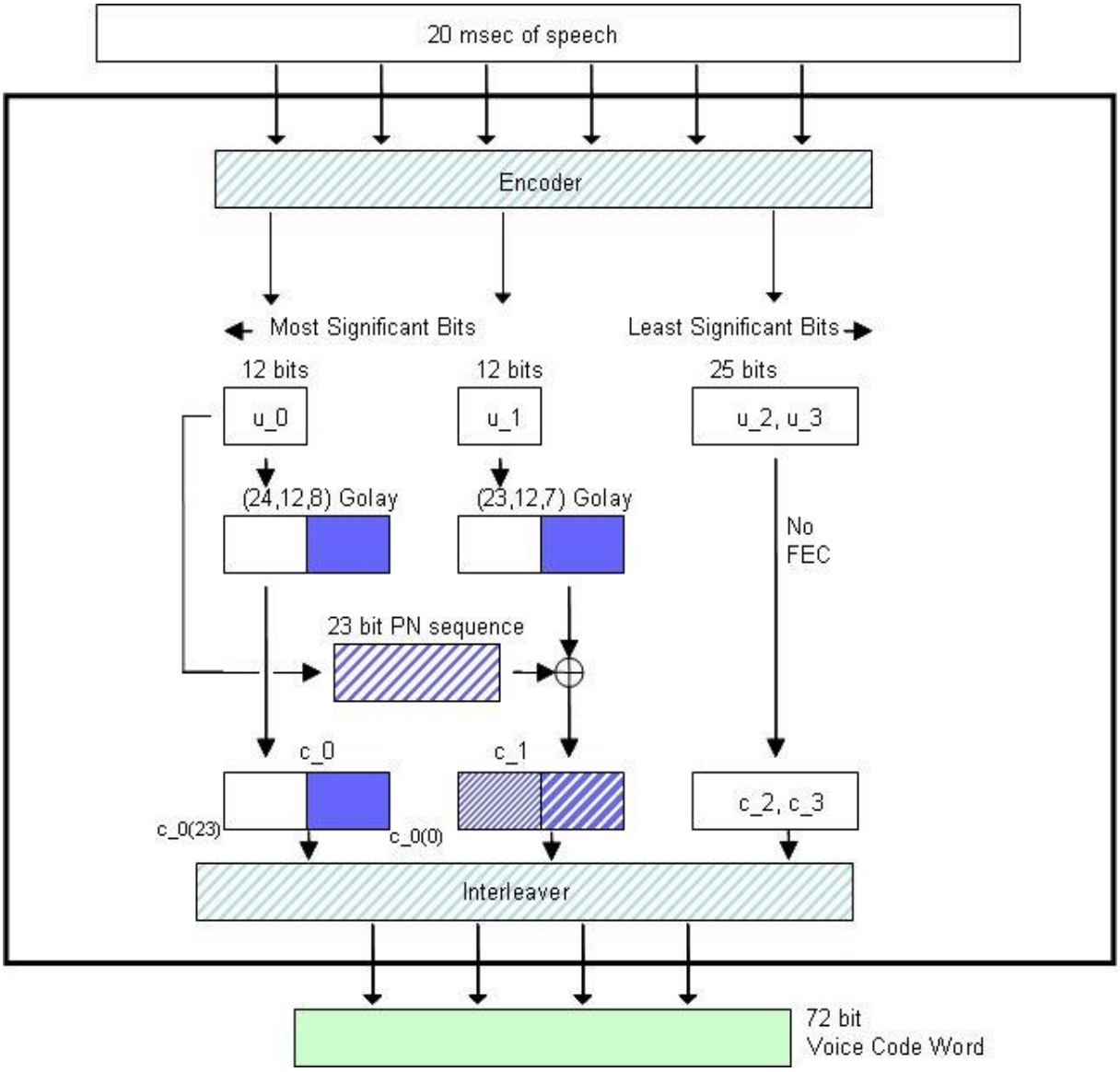
색인	비트	TX 비트
22	H(4)	TX(9)
23	PC(12)	TX(8)
24	H(3)	TX(7)
25	PC(11)	TX(6)
26	H(2)	TX(5)
27	PC(10)	TX(4)
28	H(1)	TX(3)
29	PC(9)	TX(2)
30	H(0)	TX(1)
31	PC(8)	TX(0)

음성 통화의 후발 진입을 지원하는 IV 시그널링

IV를 전달하기 위하여, FEC에 의하여 보호되지 않는 비트들 중 일부에서 보코더 비트 훔치기가 이용된다. IV 정보를 전달하는데 20 ms 보코더 프레임 마다의 4개의 보코더 비 FEC 보호 비트가 사용된다. 20 ms 보코더 프레임의 일반적인 내용은 DMR 협회의 'DMR

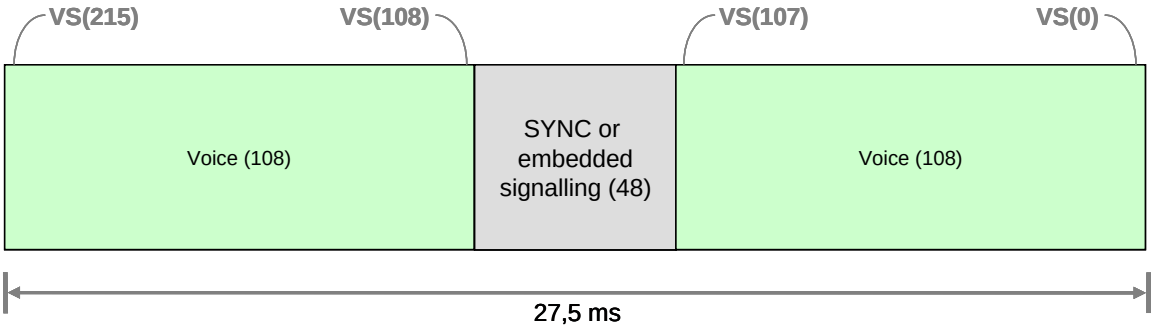
CAI Transmit Bit Order with AMBE_2 Vocoder’ 문서에 기술되어 있다.

.



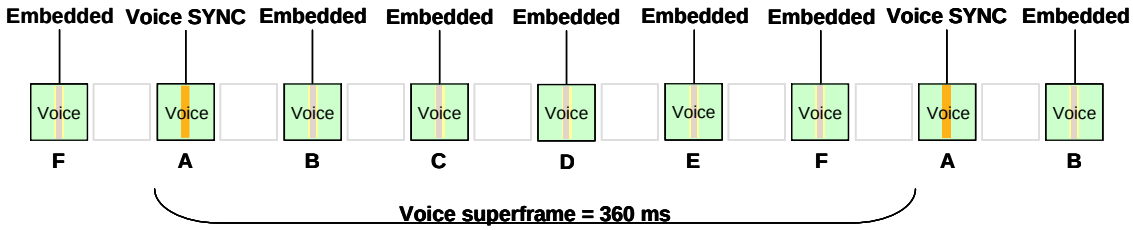
(그림 6-4) 20 ms 보코더 프레임 생성

하나의 DMR 음성 버스트 프레임은 216 비트로 구성된다. 그러므로 3 개의 20 ms 보코더 프레임 (3 x 72 비트 = 216 비트) 또는 오디오의 60 ms는 하나의 음성 버스트에 운반되며, (그림 6-5) (ETSI TS 102 361-1 6.1절의 그림 5)에 나타낸 바와 같다.



(그림 6-5) DMR 음성 버스트

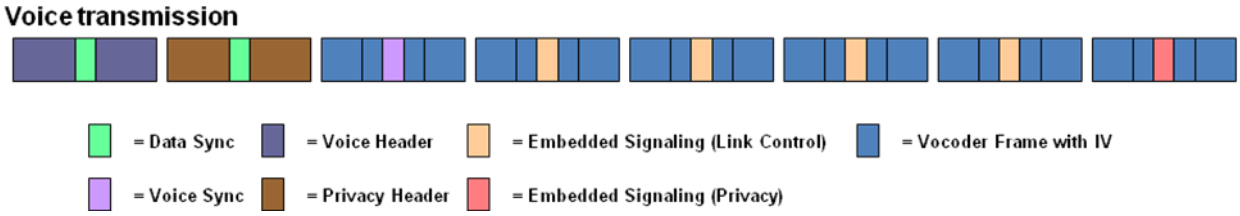
하나의 음성 수퍼 프레임은 (그림 5-6)에 나타낸 바와 같이 6 개의 DMR 음성 버스트로 구성된다. 이는 (그림 6-6)에 나타낸다.



(그림 6-6) DMR 음성 수퍼 프레임

하나의 DMR 음성 버스트가 3 개의 20 ms 보코더 프레임에 운반되므로, 수퍼 프레임은 18 개의 20 ms 보코더 프레임에 운반된다. 보코더 프레임 마다 4 비트를 훔치면 결룩 수퍼 프레임 마다 훔치는 비트는 72 비트가 될 것이다.

(그림 6-7)은 ETSI DMR 기반에 근거하고 DMR 협회에서 정제된 무선 음성 암호화 솔루션의 다양한 측면을 보여준다.



(그림 6-7) 정제된 무선 음성 암호화 솔루션의 다양한 측면

7. 데이터 암호화

<출처: ETSI TS 102 361-1 5.1.3.1절과 8.2.1.4절>

음성 전송과 달리 데이터 전송은 후발 진입을 지원하지 않는다. 따라서 전송을 시작할 때 암호화 매개변수를 전달하는 메커니즘만 필요하다. 이는 두 번째 (Proprietary) 데이터 헤더를 통해 수행된다. 두 번째 데이터 헤더의 기반은 ETSI TS 102 361-1의 5.1.3.1절

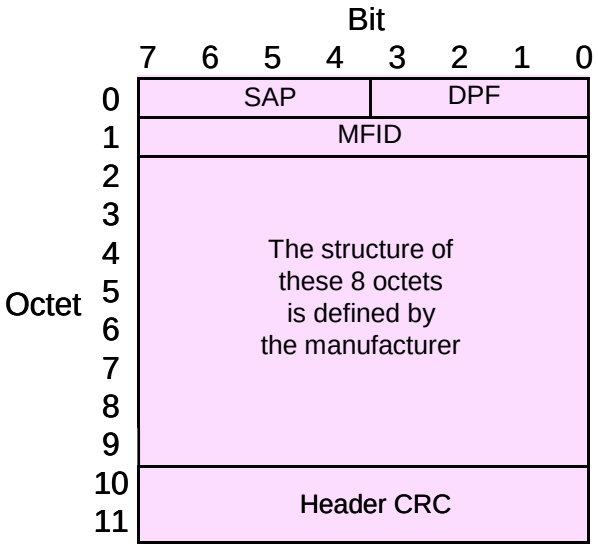
그림 5.10 및 8.2.1.4절 그림 8.6에 정의되어 있다.

(그림 7-1)은 2개의 데이터 헤더가 필요한 2개의 단말기 간의 단일 슬롯 상향 데이터 전송 교환을 나타낸다.

(그림 7-1) 이중 헤더 데이터 타이밍

7.1. Proprietary 데이터 헤더

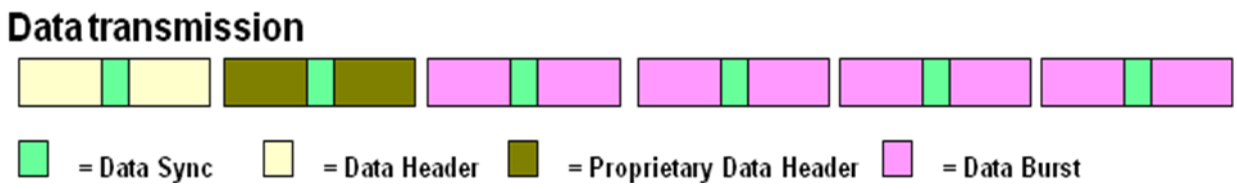
A proprietary 데이터 패킷은 모든 데이터 헤더 블록을 첫 번째 헤더 블록으로 사용한다. 두 번째 헤더 블록도 있다. 두 번째 헤더 블록의 존재는 첫 번째 헤더의 서비스 접속점 (SAP) 정보 요소의 특정 값(=9)으로 표시된다. 두 번째 헤더 블록의 구조는 (그림 7-2)에 나와 있다.



(그림 7-2) proprietary 패킷의 두 번째 헤더 블록

음성 암호화 솔루션과 마찬가지로, 데이터 암호화 솔루션은 ETSI DMR에 정의되어 있지만 그 신호에 대한 세부사항은 DMR 협회 솔루션에 나와 있다.

(그림 7-3)은 ETSI DMR 기반에 근거하고 DMR 협회에서 정제된 무선 데이터 암호화 솔루션의 다양한 측면을 보여준다



(그림 7-3) 데이터 전송

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서

- 해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.
※ 본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있으며, ETSI 원문에 대한 확약서는 ETSI 웹사이트 (https://ipr.etsi.org/)에서 확인할 수 있습니다.

부 록 Ⅰ-2

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

부 록 Ⅰ -3

본 표준의 연계(family) 표준

해당 사항 없음

부 록 Ⅰ -4

참고 문헌

해당 사항 없음

부 록 Ⅰ-5

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제 1 판	2018.xx	제정 TTAK.KO-	-	공공안전통신 프로젝트그룹 (PG902)

부 록 II

영문 번역

5 DMR Encryption

The DMR encryption defined by DMR Association and AES256 are used. And the DMR encryption has defined voice and data encryption methods are detailed in two papers;

- DMR Encryption
- ARC4 Encryption for DMR Association.

The first paper details the AES256 encryption algorithm and the second paper details how the encryption parameters are transported across the air interface. Because the voice solution is intricately linked to the AMBE +2 vocoder, the DMR Association's paper titled 'DMR CAI Transmit Bit Order with AMBE+2 vocoder' is also recommended.

Over the Air Signalling Parameters

The encryption parameters sent over the air for both voice and data are:

- Algorithm ID (3 bits, 4 defined)
- Key ID (8 bits, 255 supported)
- Initialization Vector (32 bits)

- How these parameters are transported across the air interface are different for voice and data. Details of the voice and data solutions are described in more detail below. Four encryption algorithms are currently defined in the DMR Association encryption solution, but for TTA only AES256 is supported.

Sending the Algorithm ID explicitly identifies the encryption algorithm when more than one algorithm is supported as in the DMR Association solution. However for TTA only AES256 is supported.

The Key ID is configured to represent a pre-programmed key. The actual key is not sent over the air, rather only the pre-programmed identifier. Up to 255 keys can be supported with this implementation.

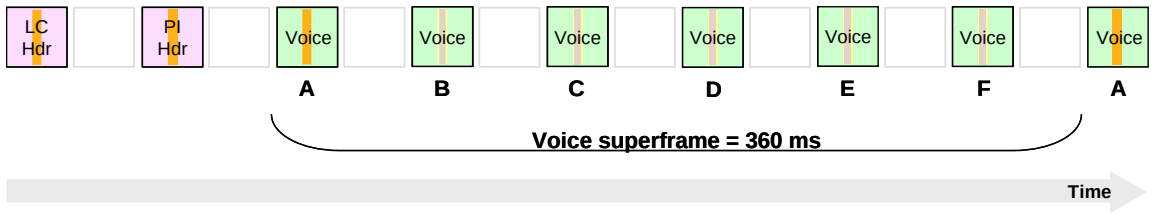
The Initialization Vector (IV) is important because it acts as a randomizer such that the encryption of the same plain text message multiple times results in different encrypted messages each time. Therefore data repetition is prevented and it is more difficult for a hacker to find patterns and ultimately break the algorithm.

6. Voice Encryption

<Source: ETSI TS 102 361-1 clause 5.1.2.1 and 6.2>

ETSI TS 102 361-1 lays the groundwork to support over the air encryption signalling. This is illustrated below in (Figure 6-1) and <Table 6-1>, which identifies a Privacy Indicator (PI) Header.

For conventional systems a voice LC header shall be sent and a PI header may be sent at the beginning of the voice transmission as illustrated in (Figure 6-1). In this case, the voice LC header shall precede the PI header.



(Figure 6-1) Voice initiation with LC and PI header

<Table 6-1> Data Type information element definitions

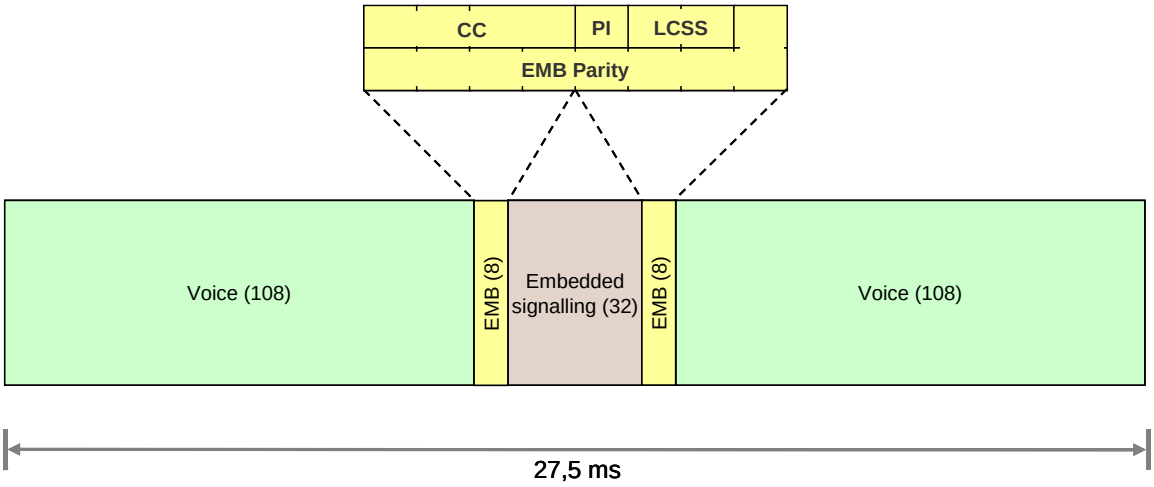
Data Type	Purpose	Payload FEC
PI Header, see note	Privacy Indicator information in a standalone burst	BPTC(196,96)
Voice LC Header	Indicates the beginning of voice transmission, carries addressing information	BPTC(196,96)
Terminator with LC	Indicates the end of transmission, carries LC information	BPTC(196,96)
CSBK	Carries a control block	BPTC(196,96)
MBC Header,	Header for multi-block control	BPTC(196,96)
MBC Continuation	Follow-on blocks for multi-block control	BPTC(196,96)
Data Header	Carries addressing and numbering of packet data blocks	BPTC(196,96)
Rate ½ Data Continuation	Payload for rate ½ packet data	BPTC(196,96)
Rate ¾ Data Continuation	Payload for rate ¾ packet data	Rate ¾ Trellis
Idle	Fills channel when no info to transmit	BPTC(196,96)
Unified Single Block Data	Carries control and/or data payload in a single block	BPTC(196,96)
NOTE: This information element is not defined in the present document and is reserved for future use.		

The NOTE in <Table 1> states the Privacy Header is not defined in ETSI DMR, however it is defined in the two DMR Association documents. This supports send the encryption information (Key ID, Algorithm ID and IV) before the voice payload as illustrated in the (Figure 6-2)

For a clear voice transmission, it is possible to late enter a call when the voice header is missed. This supported by carrying the voice header information as embedded signalling in voice bursts B – E. Late Entry functionality is also supported for encrypted voice calls by the DMR Association solution. This involves 2 separate methods. One method carries the Key ID and Algorithm ID and other method carries the IV.

Key ID and Algorithm ID signaling to support voice late entry

Embedded signaling in Voice Burst F is utilized to carry the Key ID and Algorithm ID information. (Figure 6-2) (ETSI TS 102 361-1 clause 6.2) illustrates a voice burst with embedded signaling.



(Figure 6-2): Voice burst with embedded signalling

The EMB field is further defined in ETSI TS 102 361-1 clause 9.1.2. Because the encryption parameters plus a CRC are transported by non-Reverse Channel embedded signaling in one burst, the PI bit and the LCSS bits in the EMB field are set to 0_2 and 00_2 respectively, as per ETSI TS 102 361-1 clauses 9.3.2 and 9.3.3. This is illustrated below in <Tables 6-2> and <Table 6-3> from ETSI TS 102 361-1.

<Table 6-2> Privacy Indicator

Information element	Length	Value	Remark
Pre-emption and power control Indicator	1	0_2	The embedded signalling carries information associated to the same logical channel or the Null embedded message (see note)
		1_2	The embedded signalling carries RC information associated to the other logical channel (see note)
NOTE: This is referred to Aligned channel timing (see clause 5.1.1.1); in case of Offset channel timing (see clause 5.1.1.2) both PI = 0 and PI = 1 refer to the same logical channel.			

<Table 6-3> LC Start/Stop (LCSS)

Information element	Length	Value	Remark
LC Start/Stop	2	00_2	Single fragment LC or first fragment CSBK signalling, see note
		01_2	First fragment of LC signalling
		10_2	Last fragment of LC or CSBK signalling
		11_2	Continuation fragment of LC or CSBK signalling
NOTE: There is no Single fragment LC defined for CACH signalling.			

The 32 bits of Embedded Signaling consists of a Key ID, an Algorithm ID, a CRC and FEC.

More specifics are given in the DMR Association documents, but <Table 6-4> is the general solution.

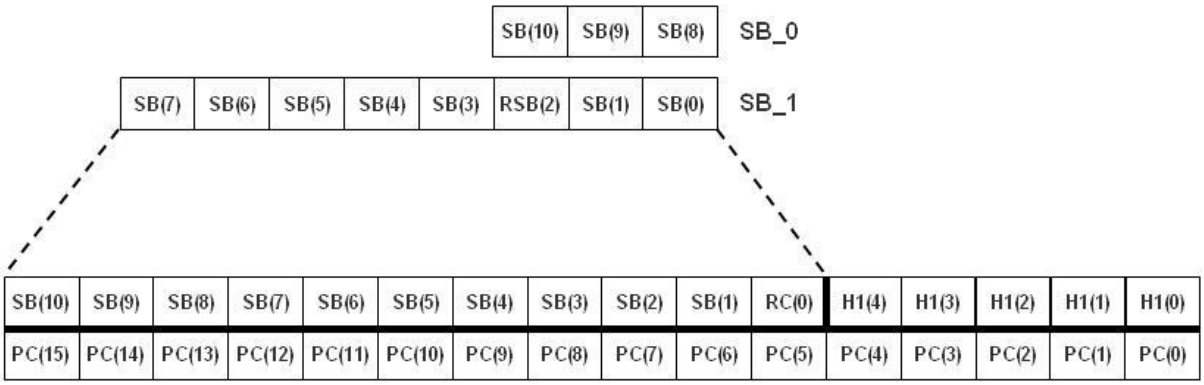
<Table 6-4> Voice Encryption Embedded Signaling Example

Information element	Length	Remark
Key ID	8	
Algorithm ID	3	
CRC and FEC	21	

Non-Reverse Channel Single Burst BPTC

<Source: ETSI TS 102 361-1 clause B.2.2.1>

The non-RC Single Burst FEC is a special case of the embedded signaling code and is used to carry the embedded Key ID and Algorithm ID information. The format for the BPTC Encode Matrix is the same as for the variable length embedded signalling. However, the interleaving is performed differently to provide additional resistance to errors over a single burst. (Figure 6-3) illustrates the encoding details for non-RC Single Burst signalling. The 11 bits of non-RC Single Burst signalling, SB(10) - SB(0) are placed in the first row of the matrix and protected with a Hamming (16,11,4) code. The bottom row contains an even parity check bit for each column. In this case, the parity check row is identical to the information row.



(Figure 6-3) Format for non-Reverse Channel Single Burst

The first step in interleaving the bits for the transmission is to sequentially number the bits of the FEC encoded matrix from top-to-bottom, left-to-right. <Table 6-4> lists the bits of the Encoder Matrix along with their corresponding indices. Each bit is then assigned a new index in the interleaved array where:

$$\text{Interleave Index} = \text{Index} \times 17 \text{ modulo } 32$$

The value of the Interleave Index determines the location of each bit in the transmission array,

which is placed in the embedded field.

<Table 6-5> Interleaving indices for non-Reverse Channel Single Burst

Bit	Index	Interleave Index	Bit	Index	Interleave Index	Bit	Index	Interleave Index
SB(10)	0	0	PC(10)	11	27	H(4)	22	22
PC(15)	1	17	SB(4)	12	12	PC(4)	23	7
SB(9)	2	2	PC(9)	13	29	H(3)	24	24
PC(14)	3	19	SB(3)	14	14	PC(3)	25	9
SB(8)	4	4	PC(8)	15	31	H(2)	26	26
PC(13)	5	21	SB(2)	16	16	PC(2)	27	11
SB(7)	6	6	PC(7)	17	1	H(1)	28	28
PC(12)	7	23	SB(1)	18	18	PC(1)	29	13
SB(6)	8	8	PC(6)	19	3	H(0)	30	30
PC(11)	9	25	SB(0)	20	20	PC(0)	31	15
SB(5)	10	10	PC(5)	21	5			

<Table 6-5> lists the bit ordering after interleaving. The index values 0 to 31 correspond to the Interleave Index from the previous table. The resulting array contains 32 bits, numbered from TX(31) down to TX(0) for placement in the embedded field.

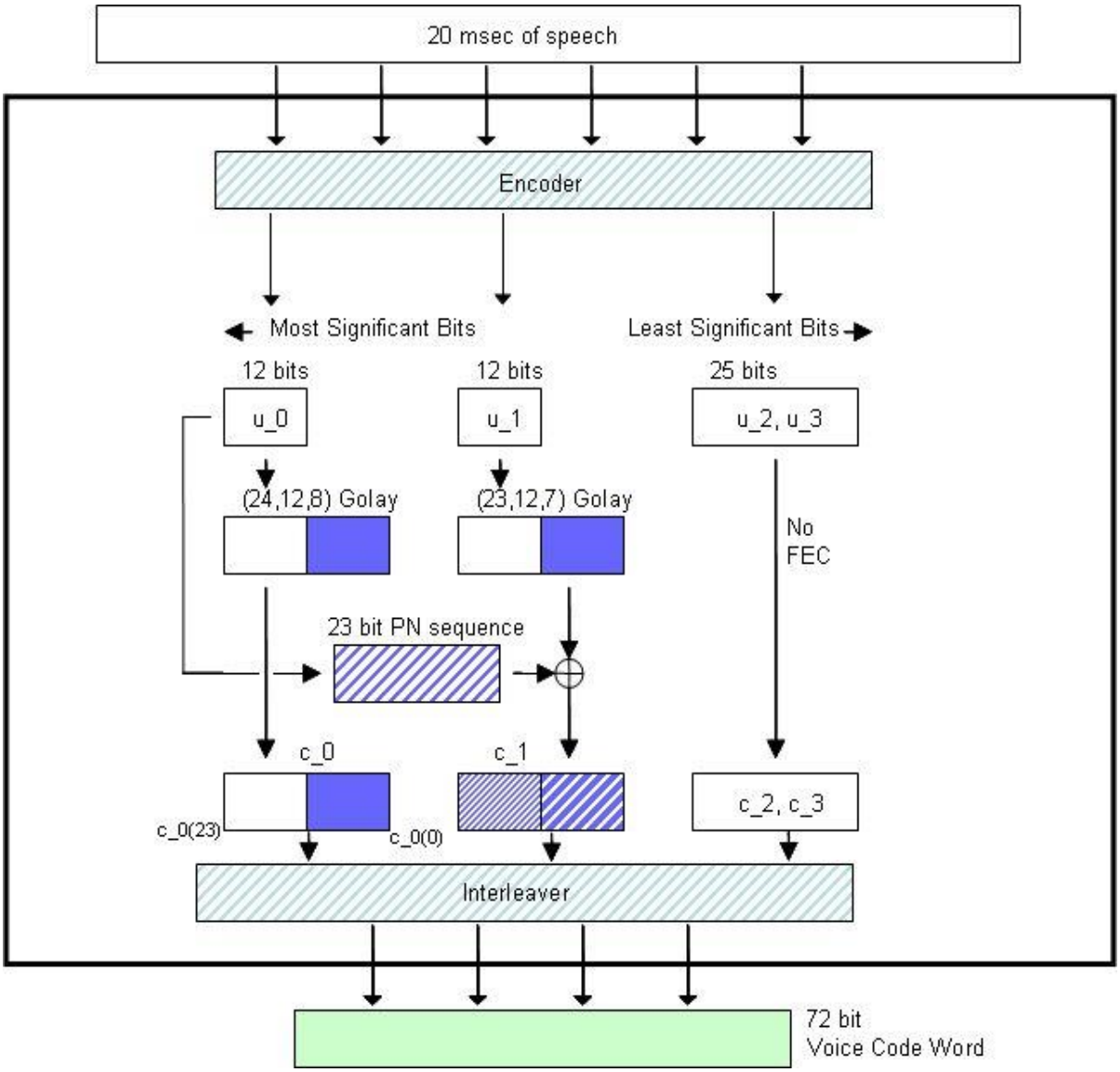
<Table 6-6> Transmit bit ordering for non-Reverse Channel Single Burst

Index	Bit	TX Bit	Index	Bit	TX Bit	Index	Bit	TX Bit
0	SB(10)	TX(31)	11	PC(2)	TX(20)	22	H(4)	TX(9)
1	PC(7)	TX(30)	12	SB(4)	TX(19)	23	PC(12)	TX(8)
2	SB(9)	TX(29)	13	PC(1)	TX(18)	24	H(3)	TX(7)
3	PC(6)	TX(28)	14	SB(3)	TX(17)	25	PC(11)	TX(6)
4	SB(8)	TX(27)	15	PC(0)	TX(16)	26	H(2)	TX(5)
5	PC(5)	TX(26)	16	SB(2)	TX(15)	27	PC(10)	TX(4)
6	SB(7)	TX(25)	17	PC(15)	TX(14)	28	H(1)	TX(3)
7	PC(4)	TX(24)	18	SB(1)	TX(13)	29	PC(9)	TX(2)
8	SB(6)	TX(23)	19	PC(14)	TX(12)	30	H(0)	TX(1)
9	PC(3)	TX(22)	20	SB(0)	TX(11)	31	PC(8)	TX(0)
10	SB(5)	TX(21)	21	PC(13)	TX(10)			

IV signaling to support voice late entry

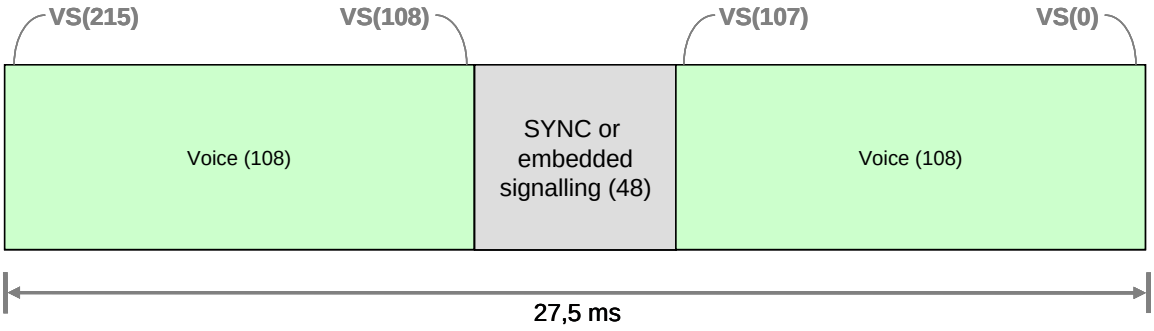
To carry the IV, vocoder bit stealing is utilized on some of the bits that are not protected by

FEC. Four vocoder non-FEC protected bits of every 20 ms vocoder frame are used to carry the IV information. The general contents of a 20 ms vocoder frame is illustrated in (Figure 6-4> from DMR Association's 'DMR CAI Transmit Bit Order with AMBE_2 Vocoder'.



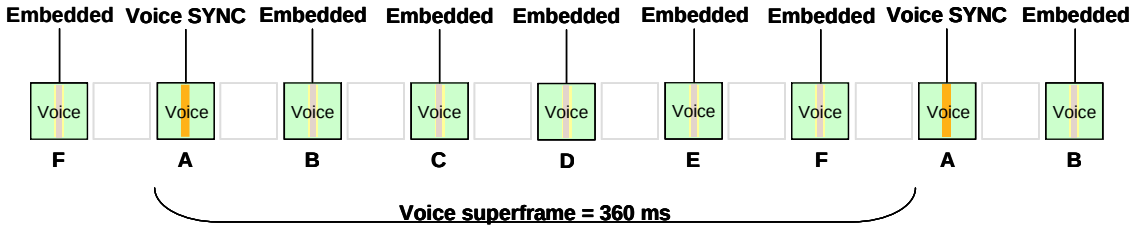
(Figure 6-4) 20 ms Vocoder Frame Construction

One DMR voice burst frame carries 216 bits. Therefore 3 20 ms vocoder frames (3 x 72 bits = 216 bits) or 60 ms of audio is carried in one voice burst. This is illustrated in (Figure 6-5) from ETSI TS 102 361-1 clause 6.1.



(Figure 6-5) DMR Voice Burst

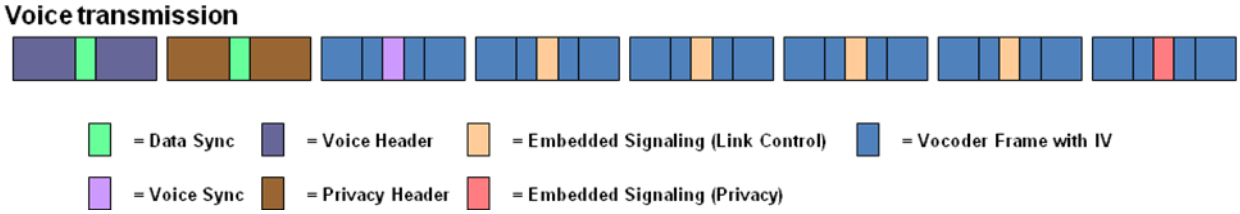
One voice superframe consists of 6 DMR voice bursts. This is illustrated in Figure 6 from ETSI TS 102 361-1 clause 5.1.2.1.



(Figure 5-6) DMR Voice Superframe

Since one DMR voice burst carries 3 20 ms vocoder frames then a superframe contains 18 20 ms vocoder frames. Stealing four bits per vocoder frame results is 72 stolen bits per superframe. These 72 carry the IV, a CRC and FEC.

(Figure 5-7) illustrates the different aspects of the over the air voice encryption solution, that is based upon an ETSI DMR foundation and refined within the DMR Association.



<Figure 5-7) Different Aspects of the Over the Air Voice Encryption Solution

7. Data Encryption

<Source: ETSI TS 102 361-1 clause 5.1.3.1 and clause 8.2.1.4>

Unlike voice transmissions, data transmissions do not support late entry. Therefore only a mechanism to carry the encryption parameters at the beginning of the transmission is required. This is accomplished via a second (proprietary) data header. The foundation for the second data header is defined in ETSI TS 102 361-1 clause 5.1.3.1, figure 5.10 and clause 8.2.1.4,

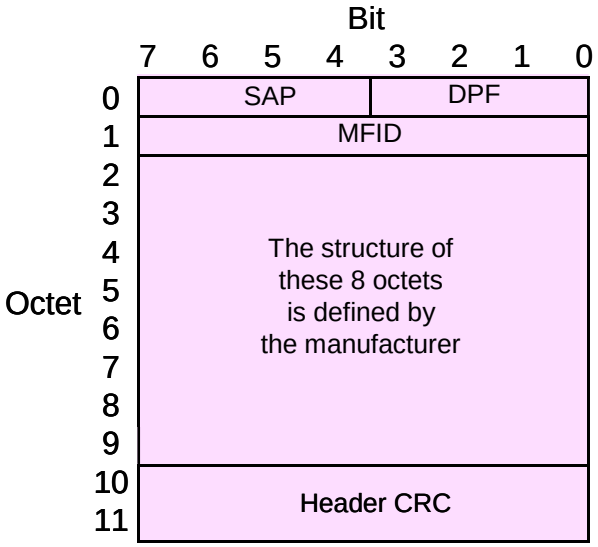
figure 8.6.

(Figure 7-1) illustrates a single slot inbound data transmission exchange between two MS for which two data headers are required.

(Figure 7-1) Dual header data timing

6.1. Proprietary data header

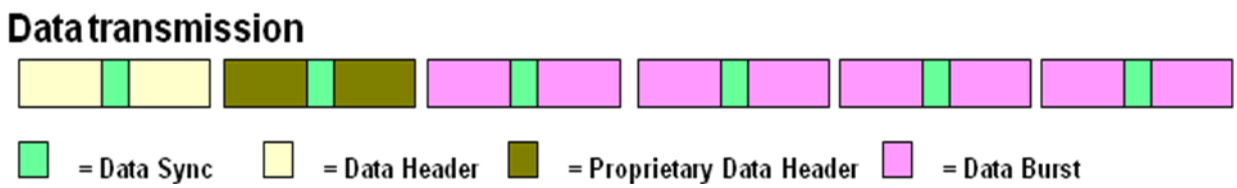
A proprietary data packet uses any data header block as its first header block. It also has a second header block. The presence of second header block is indicated by the specific value (= 9) of the Service Access Point (SAP) information element of the first header. The structure of the second header block is shown in the (Figure 7-2).



(Figure 7-2) Second header block of a proprietary packet

Similar to the voice encryption solution, the data encryption solution is defined in ETSI DMR but the signalling specifics are found in the DMR Association solution.

(Figure 7-3) illustrates the different aspects of the over the air data encryption solution, that is based upon an ETSI DMR foundation and refined within the DMR Association.



(Figure 7-3) Data Transmission

Declaration on IPR

- No IPR to be declared.