일반논문 (Regular Paper)
방송공학회논문지 제31권 제1호, 2026년 1월 (JBE Vol.31, No.1, January 2026)
https://doi.org/10.5909/JBE.2026.31.1.94
ISSN 2287-9137 (Online) ISSN 1226-7953 (Print)

OFDM 기반 DQPSK 변조를 이용한 음파통신

박 찬 휘[a)], 김 영 길[a)‡]

Acoustic Communication Using OFDM-based DQPSK Modulation

ChanHwi Park[a)] and YoungGil Kim[a)‡]

요 약

Orthogonal frequency division multiplexing (OFDM) 기반 differential quadrature phase shift keying (DQPSK) 변조 기법을 사용하여 RSA-2048 비대칭 키 암호 시스템을 적용한 암호문을 송·수신하는 음파통신 시스템을 설계하며, 이를 안드로이드 스마트폰에 실제 모뎀으로 구현한다. 통신 신호는 17 kHz ~ 19.71 kHz 주파수 대역을 이용하며, 전체 2.5초 길이에 이른다. 48 kHz 샘플 주파수로 동작하는 이 통신 시스템은, 한 번의 신호 발생으로 372 바이트를 보낼 수 있어, RSA-2048 암호 시스템 암호문의 크기 256 바이트를 보낼 수 있다. 이러한 암호문 통신을 이용해 결제 정보 및 비밀번호를 비롯한 다양한 비밀 정보를 송·수신할 수 있다.

Abstract

We design an acoustic communication system that transmits and receives encrypted messages using an RSA-2048 asymmetric key cryptosystem with orthogonal frequency division multiplexing (OFDM)-based DQPSK modulation. This system is implemented as an actual modem on an Android smartphone. The communication signal utilizes the 17 kHz to 19.71 kHz frequency band and has a total duration of 2.5 seconds. Operating at a 48 kHz sampling frequency, this communication system can transmit 372 bytes per signal generation, enabling the transmission of the 256-byte ciphertext size of the RSA-2048 cryptosystem. This ciphertext communication can be used to transmit and receive various confidential information, including payment details and passwords.

Keyword : Acoustic Communication, Android, DQPSK, OFDM

a) 서울시립대학교 전자전기컴퓨터공학부(University of Seoul)
‡ Corresponding Author : 김영길(YoungGil Kim)
E-mail: ygkim72@uos.ac.kr
Tel: +82-2-6490-2340
ORCID: https://orcid.org/0000-0001-7066-0555
※ This work was supported by the 2023 sabbatical year research grant of the University of Seoul.
· Manuscript November 17, 2025; Revised January 6, 2026; Accepted January 6, 2026.

Ⅰ. 서 론

LTE, NR, Wi-Fi, 블루투스 등의 전자기파를 이용한 무선 통신 기술은 데이터 무선 교환을 위한 핵심 기술로 널리 사용되고 있다. 그러나 이러한 기술은 전용 RF 하드웨어가 장착되어야만 통신이 가능하다. 반면, 음파통신은 스피커와 마이크, 그리고 디지털 연산 장치만을 필요로 하는 통신

기술로, 전용 RF 하드웨어가 장착되지 않은 기기에서도 소프트웨어 설치를 통해 스피커와 마이크만으로 간단히 무선 통신을 가능하게 할 수 있다는 장점이 있다. 이에, 다양한 디지털 시스템에서 통신 기능을 즉시 적용할 수 있다. 이러한 시스템은 IoT 장치, 결제 단말기, 웨어러블 장치, 기타 가전 기기 등 다양한 장치를 아우른다. 그 가운데, 스마트폰은 음파통신에 필요한 스피커와 마이크를 모두 장착하고 있고, 고속 연산 능력을 갖추고 있으며, 널리 보급되어 있다는 점에 있어 음파통신에 적합한 디지털 시스템이다.

음파통신은 1:1 통신이 가능할 뿐 아니라, 음파의 방사하는 특성으로 인해 음파를 수신한 모든 기기에 데이터를 전송하는 1:N 브로드캐스팅 통신 또한 가능하다. 반면에, 이 음파의 방사 특성으로 인해 제삼자에 의한 평문 도청 위험이 존재한다. 더욱이 음파 신호는 녹음과 재생이 간단하므로, 평문 암호화의 필요성이 드러나고 있다.

이 논문이 제시하는 핵심 목표는 가청 주파수 대역을 활용한 안드로이드 운영체제 기반, 통신의 보안을 고려한 단방향 음파통신 시스템을 제시하며 구현하는 것이다.

이에 따라 다양한 제약 조건이 나타난다.

1) 통상 전자기기의 스피커·마이크는 44,100 Hz 또는 48,000 Hz의 샘플 주파수로 동작한다. 이러한 음향 기기들은 22,050 Hz, 24,000 Hz 이내 가청 주파수 대역에서 정상 작동한다. 따라서 이를 넘어서는 초음파 대역을 사용할 수 없다.
2) 단방향 통신은 수신기가 통신 데이터 오류를 감지했을 때, 송신기에 재전송 요청을 할 수 없는 특성을 가진다. 이러한 통신 오류에 대응하여, 리드 솔로몬 부호[2]를 적용한다. 이를 적용하여 정보의 부호화·복호화를 수행하여, 통신 도중 발생한 데이터 오류를 수신기에서 자체 정정할 수 있도록 한다. 리드 솔로몬 부호는 버스트 오류에 강한 특성이 있다.
3) 음파는 전문 장비 없이도 손쉽게 녹음하여 재사용할 수 있다. 통신 데이터 오용·탈취를 방지하기 위해 비대칭 키 암호화 기술인 RSA[2]를 적용한다. RSA 암호는 2030년까지 최소 2,048 비트 크기의 키를 권장한다. 이에 따라, 한 번의 통신으로 전송되는 메시지의 크기가 최소 256 바이트이어야만, 수신기가 평문으로 이를 복호할 수 있다.

스마트폰 간 음파통신은, Amplitude Shift Keying (ASK) 및 Frequency Shift Keying (FSK) 기반[3], 시간에 따라 주파수가 천이하는 처프 신호를 이용한 방식[4], 파일럿 톤을 사용하는 OFDM 기반의 PSK 변조[5] 그리고 Direct Sequence Spread Spectrum (DSSS) 방식[6] 등이 있다. FSK, Chirp 변조는 대역폭을 매우 과다하게 사용하는 기법이다. 즉, 이 두 가지 기법은 수신단의 복조를 쉽게 해주는 장점이 있지만, 대역 효율성 (spectral efficiency)이 작은 것으로 알려져 있다[10]. DSSS는 [6]에 나오는 기법인데 처리 이득 16을 갖기 위해 94.5 bps로 데이터 속도가 매우 작다. 따라서, FSK, Chirp, DSSS 모두 암호화된 데이터를 전송하기 위한 고속 통신에 적합하지 않다.

관련 연구는 20 kHz 이상의 초음파 대역 또는 20 kHz에 근접한 가청 주파수 대역 사용을 권장한다. 이는 가청 대역에서 통신 신호가 사람의 청각에 인지될 수 있기 때문이다. Fletcher와 Munson의 등청감곡선은 동일한 에너지를 가진 음파 신호에 대한 인체의 청각 반응이 주파수에 따라 다름을 보여준다[7]. 이에 따르면, 인체의 청각은 1 kHz에서 10 kHz 사이의 음파 신호에 가장 예민하게 반응한다. 따라서 10 kHz 이상의 근 초음파 대역을 활용하면, 음파통신 신호가 인체 감각에 덜 인지되어, 감각 자극에 의한 사용자의 불쾌감을 낮출 수 있다.

그러나 [3]의 연구는 스마트폰에서 19.7 kHz 이상의 주파수를 활용한 통신에 어려움이 있음을 보인다. 이러한 초음파 대역에서 일반 소비자용 하드웨어가 보이는 응답 감쇄 특성은, 스마트폰에서 20 kHz보다 높은 초음파를 사용한 통신의 어려움을 보인다. 또한, 안드로이드 운영체제는 2015년에 발표된 안드로이드 버전 6.0 (마시멜로) 이후로 192 kHz 샘플링 주파수를 지원하지만, 실제 하드웨어가 이를 지원하지 않는다면 48 kHz보다 높은 샘플링 주파수의 사용을 권장하지 않는다[6]. 이 논문에서는 이러한 하드웨어 및 인체의 청각 인지 특성을 고려하여, 48 kHz 샘플링 주파수에서 17 kHz ~ 19.71 kHz 대역으로 동작하는 가청 대역 음파통신 시스템을 보인다.

음파는 방사하는 특징이 있어 제삼자의 통신 신호 도청 위험이 존재한다. 더욱이 음파통신 신호는 RF 전파통신과

달리, 누구나 전문 장비 없이 통신 신호를 손쉽게 녹음하고 재생할 수 있다는 보안 문제가 있다. 이렇게 녹음된 신호는 일반 스피커를 이용해 간단히 재생성될 수 있으며, 이에 보안 문제가 발생할 수 있다. 암호화 방식으로는 AES, TDES, RSA 등이 있으며, 이 가운데 RSA는 비대칭 키 알고리즘으로, AES와 TDES보다 큰 블록 크기를 요구한다[2]. 64 비트의 블록 크기를 가지는 TDES와 128 비트의 블록 크기를 가지는 AES와 달리, 키의 크기가 2,048 비트인 RSA 비대칭 키 암호화의 블록 크기는 2,048 비트이다. 즉, 송신기에서 256 바이트 암호문 메시지가 온전히 수신기로 전파되어야만 수신기에서 이를 평문으로 복호할 수 있다. 이 논문에서는 RSA-2048 암호 시스템의 블록 크기를 고려하여, 최대 372 바이트 정보를 송·수신하는 음파통신을 보인다.

제한된 통신 대역에서 대용량의 정보를 송·수신하기 위해 orthogonal frequency division multiplexing (OFDM)을 적용한다. OFDM은 다수의 서브캐리어를 효율적으로 배치해 주파수 자원의 효율을 높인다[9]. 변조 방식으로는 differential quadrature phase shift keying (DQPSK)을 적용하여, 파일럿 톤 없이 인접 심볼 간의 위상 차이만을 통해 데이터를 전송하도록 한다[10]. 이는 실제 데이터 전송과 무관한 파일럿 서브캐리어를 제거하여, 통신 대역의 효율을 높이는 장점이 있다. 대역폭이 매우 좁기 때문에 데이터 속도가 낮고, zero crossing에 따른 문제가 심각하지 않다고 판단하였다. 따라서 복잡도가 높은 π/4 offset DQPSK를 사용하지 않았다. 또한 휴대폰에서 소프트웨어를 가지고 OFDM 복조의 복잡도가 과다하여 더 간단한 DQPSK를 사용하였다. DQPSK는 음파통신에는 처음 제안하였으며, 그 이유는 음파통신에 가장 많이 사용되는 FSK가 지나치게 대역을 많이 차지하기 때문이다.

[4], [6]의 연구는 다중경로로 인한 리버브 현상이 음파통신의 주된 도전 과제임을 보인다. 다중경로에 의한 지연 확산으로 통신 오류가 발생할 수 있다. 이 통신 시스템은 핸드셰이킹 기법을 사용할 수 없는 단방향 통신이기 때문에, 송신 단말기는 수신기가 어떠한 데이터를 수신하였는지 알 수 없다. 이에 리드 솔로몬 코드를 사용하여 오류 정정 기능을 적용하였다.

이 논문은 다음과 같이 구성되어 있다. 2장은 시스템 모델을 제시한다. 3, 4장에서는 음파통신 송·수신 시스템 설계를 보인다. 5장에서는 안드로이드 스마트폰을 이용하여 구현한 결과를 보인다. 6장에서 결론을 맺는다.

II. 시스템 모델

사람이 거의 들을 수 없는 주파수인 17,000 Hz ~ 19,713 Hz가 통신에 사용되었고 OFDM에서 각 서브캐리어의 변조 기법은 DQPSK를 사용하였다. 오류 정정을 위하여 RS 부호가 사용되었으며 이 오류정정부호의 파라미터는 (1023, 298)이다. 이 논문에서 사용된 다른 파라미터들은 표 1과 같다. 전체 통신 신호 길이는 실제 사용 환경에서 과도한 지연이 발생하지 않도록 2.5초로 설정하였다. 전체 통신 신호는 동기화를 위한 0.5초 길이의 프리앰블과 4개의 0.5초 데이터 심볼로 구성된다. 제한된 주파수 대역과 시간 자원 내에서 모든 데이터 비트를 전송하기 위하여, 1,280개의 서브캐리어를 사용하였다. 여기에 DPSK 복조를 위한 기준 위상 정보를 가지는 1개의 서브캐리어와, 도플러 효과로 의

표 1. 시스템 파라미터
Table 1. System Parameters

Sampling Frequency (f_s)	48,000 Hz
Quantization levels	16 bit
Modulation for Subcarriers	DQPSK
Subcarrier Spacing	2.105 Hz
Number of Subcarriers ($n_{subcarriers}+2$)	1,282
Lowest Frequency (f_l)	17,000 Hz
Highest Frequency (f_h)	19,713 Hz
Error Correction Code (Reed Solomon(n_{rs}, k_{rs}))	RS(1023, 298)

한 주파수 천이를 감지하기 위한 1개의 서브캐리어를 추가하여, 총 1,282개의 서브캐리어를 사용하였다.

Ⅲ. 음파통신 모뎀 설계

1. 송신기 구조

10,240 비트의 데이터 $c'[n]$은 2,560 비트 4부분으로 나뉘어, 각 2,560 비트가 순차대로 2 비트로 재구성되어 $d_k[n]$에 할당된다. 즉, $d_0[n]$은 $[m_0, m_1, \dots m_{255}]$의 정보를, $d_1[n]$은 $[m_{256}, m_{257}, \dots, m_{297}, p_0, p_1, \dots, p_{213}]$의 정보를, $d_2[n]$은 $[p_{214}, p_{215}, \dots, p_{469}]$의 정보를, $d_3[n]$은 $[p_{470}, p_{471}, \dots, p_{724}, 0]$의 정보를 2 비트 배열의 형태로 가진다.

각 $d_k[n]$은 다음 식이 나타내는 그레이 코드 변환 과정을 거친다.

$$g_k[n] = \begin{cases} 0 \, (d_k[n] = 0) \\ 1 \, (d_k[n] = 1) \\ 3 \, (d_k[n] = 2) \\ 2 \, (d_k[n] = 3) \end{cases} \quad (1)$$

수신기가 차분에 따른 복조를 수행할 수 있도록, 송신기는 데이터에 누산 연산을 가한다. 누산 연산의 초깃값은 0으로써, 다음과 같다.

$$a_k[n] = \begin{cases} 0 & (n = 0) \\ (a_k[n-1] + g_k[n-1]) \bmod 4 & (n > 0) \end{cases} \quad (2)$$

이 누산 데이터 $a_k[n]$에 대해, 다음과 같이 4진 위상 변조 심볼을 구성한다.

$$D_k[n] = \begin{cases} +1+0i \, (a_k[n] = 0) \\ +0+1i \, (a_k[n] = 1) \\ -1+0i \, (a_k[n] = 2) \\ +0-1i \, (a_k[n] = 3) \end{cases} \quad (3)$$

$D_k[n]$은 DQPSK 심볼 데이터로써, 오로지 인접 자료의 위상 차이에만 유효한 정보가 있다.

OFDM은 서로 직교하는 주파수에 변조된 심볼을 할당함으로써 대역 효율을 높여 비트 전송률을 높이는 기법으로, 그 방식은 다음과 같다.

$$O(t) = \sum_{k=0}^{N-1} X_k e^{\frac{i2\pi kt}{T}} \; (0 \le t < T) \quad (4)$$

$$s(t) = \mathcal{R}\left\{ O(t) e^{i2\pi f_c t} \right\} \quad (5)$$

위 수식에 있어서, X_k는 변조된 심볼이며, N은 서브캐리어의 개수, T는 OFDM 심볼 길이, f_c는 캐리어 주파수이다. 각 서브캐리어는 $\frac{1}{T}\,[Hz]$만큼의 간격으로 떨어져 있으므로, 각 서브캐리어는 직교하며, 다른 서브캐리어와 구분이 가능하다. 따라서 식 (4)를 통해 OFDM 기반의 기저대역 신호를 만들 수 있으며, 식 (5)를 이용해 통신 주파수로 변조하여, 실제 송신할 수 있는 신호를 만들 수 있다.

이 논문이 목표로 하는 17 kHz ~ 19.71 kHz 주파수 대역의 음파통신 신호는 48 kHz 샘플 주파수 시스템에서 기저대역 신호와 통신 신호 모두 샘플 단위의 디지털 처리가 가능하다. 따라서 디지털 신호처리 환경에서 연산의 효율을 최적화하기 위해, 기저대역 신호 생성과 통신 주파수로의 주파수 천이를 동시에 수행한다. 이에 먼저 기저대역 신호 $B_k[n]$를 다음과 같이 보인다.

$$B_k[n] = \begin{cases} +2+0i & (n = 0) \\ D_k[n - n_{doppler}] & (n \ge n_{doppler}) \end{cases} \quad (6)$$

$n = 0$에서 $B_k[n]$는 주파수 오프셋 서브캐리어를 가진다. 통신 신호가 도플러 효과에 의해 주파수가 천이할 경우, 수신기는 이 주파수 오프셋 서브캐리어의 주파수 천이를 감지하여 이를 보상하는 역할을 수행한다. 도플러 서브캐리어는 다른 서브캐리어와의 간섭을 최소화하기 위해, 다른 서브캐리어와 $n_{doppler}$ 샘플만큼 떨어져 있다. 그림 1에 주파수 영역에서 나타낸 OFDM 기반 DQPSK 기저대역 신호를 나타냈다. 그림 1 (a)는 크기 정보를 보이며, 그림 1 (b)는 위상 정보를 보인다.

다음으로, 이 기저대역 신호를 통신 주파수로 주파수 천이한다. 이를 위해, 통신 주파수의 주파수 bin 정보가 필요

하다. 길이 n_{dft}에 대한, 정규화된 통신 하단 경계 주파수 k_l는 다음과 같다.

$$k_l = \left\lfloor \frac{n_{dft} * f_l}{f_s} \right\rfloor \tag{7}$$

n_{dft} 길이 복소수 배열의 역 푸리에 변환 결과가 실수 배열이 되기 위해서, 인덱스 $n = n_{dft}/2$ 기준으로 그 복소수 배열의 크기는 우함수이며 위상은 기함수이어야 한다. 이에 따라 n_{dft} 길이를 가지는 $O_k[n]$을 다음과 같이 정의한다.

$$O_k[n] = \begin{cases} B_k[n-k_l] & (k_l \le n < \frac{n_{dft}}{2}) \\ Conj\{O_k[n_{dft}-n]\} & (\frac{n_{dft}}{2} < n < n_{dft}) \end{cases} \tag{8}$$

이에 따라 생성된 $O_k[n]$을 그림 2에 나타냈다. 그림 2 (a)는 $O_k[n]$의 크기를 나타내며, 그림 2 (b)는 $O_k[n]$의 위상을 나타낸다.

이어서, $O_k[n]$에 푸리에 역변환 연산을 수행하면, 통신 주파수로 변조된 신호를 구할 수 있다. 실제 연산 장치에서의 푸리에 역변환은, 부동소수점 정밀도의 한계로 인해 허

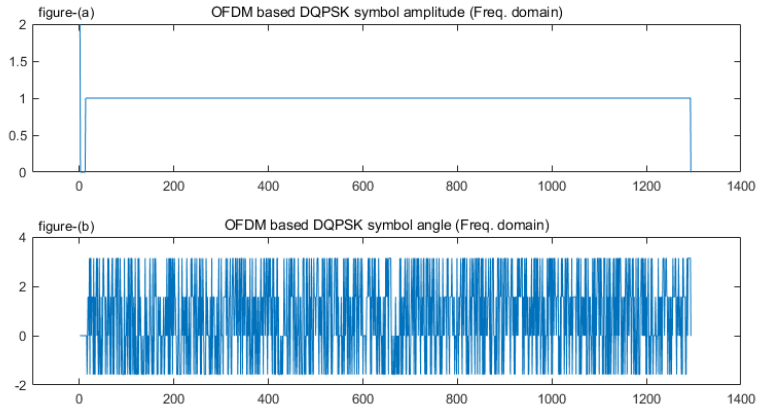

그림 1. (a) 주파수 영역에서 나타낸 기저대역 신호의 진폭 (b) 주파수 영역에서 나타낸 기저대역 신호의 위상

Fig. 1. (a) Magnitude of baseband signal in frequency domain (b) Phase angle of baseband signal in frequency domain

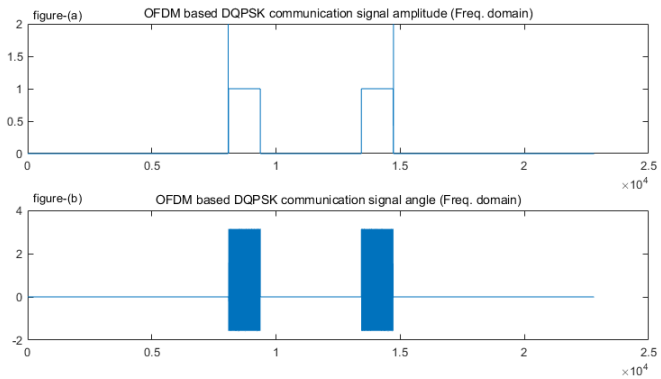

그림 2. (a) 주파수 영역에서 나타낸 RF 대역 신호의 진폭 (b) 주파수 영역에서 나타낸 RF 대역 신호의 위상

Fig. 2. (a) Magnitude of passband signal in frequency domain (b) Phase angle of passband signal in frequency domain

수부가 정확히 0이 되지 않고, 매우 작은 값을 보인다. 이에 따라, 푸리에 역변환 연산 결과의 실수부만을 취한다.

$$o_k[n] = \mathcal{R}\{IDFT\{O_k[n]\}\} \tag{9}$$

OFDM은 다중경로에 의한 심볼 사이 간섭 (Inter Symbol Interference: ISI)의 영향으로, 서브캐리어의 직교성 훼손 현상을 줄이기 위해, Cyclic Prefix (CP)를 이용한다. CP는 OFDM 푸리에 심볼의 일부를 복사 및 전치 삽입하여, 다중경로에 의해 발생한 이전 OFDM 심볼 잔향 성분을 줄이는 역할을 한다[9].

음파통신은 스피커를 신호 발생 장치로 이용한다. 스피커는 물리적으로 움직이는 진동판을 통해 음파를 발생시키는데, 입력 시퀀스의 인접 샘플 사이에 큰 불연속이 나

$$x_k[n] = \begin{cases} o_k[n_{dft}-n] \bullet 2n/n_{cp} & (n \geq 0, n < n_{cp}/2) \\ o_k[n-n_{cp}/2] & (n \geq n_{cp}/2, \\ & \quad n < n_{symbol}-n_{cp}/2) \\ o_k[n-(n_{symbol}-n_{cp}/2)] & (n \geq n_{symbol}-n_{cp}/2, \\ \quad \bullet\ 2(n_{symbol}-n-1)/n_{cp} & \quad n < n_{symbol}) \end{cases} \tag{10}$$

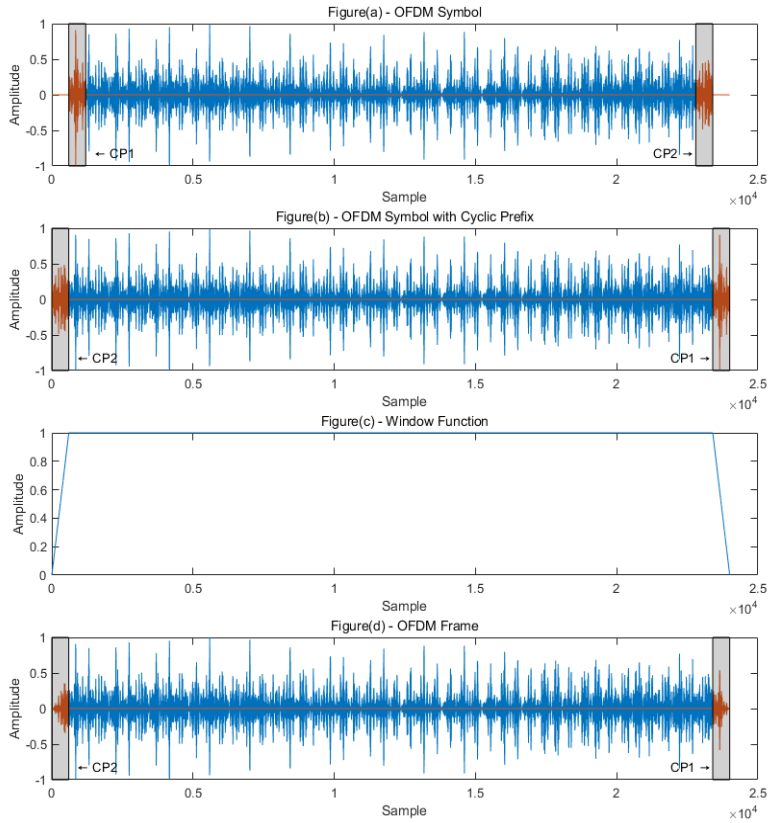

그림 3. (a) 시간 영역에서 OFDM 신호 (b) CP를 추가한 경우 시간 영역에서 OFDM 신호 (c) 윈도우 함수 (d) 윈도우 함수가 적용된 OFDM 신호
Fig. 3. (a) OFDM signal in the time domain (b) OFDM signal after addition of CP in the time domain (c) window function (d) OFDM signal after applying window function

타날 경우, 클릭 노이즈가 발생할 수 있다[12]. 이 클릭 노이즈는 통신 대역을 넘어서는 넓은 주파수 영역에 에너지를 가지며, 통신 사용자에게 잡음으로 인지될 수 있어, 통신 품질을 저하하는 요인으로 작용하므로 제거가 필요하다. 이러한 클릭 노이즈를 방지하기 위해 다음과 같은 CP를 설계하였다.

이 CP를 적용한 OFDM 심볼은 다른 OFDM 심볼과의 접점에서 항상 0의 값을 가지며 인접한다. 이에 샘플 사이에 불연속이 발생하지 않으며, 클릭 노이즈로 인한 잡음을 방지할 수 있다. 이러한 CP를 적용할 경우, OFDM 심볼에 변형을 가하지 않으면서 클릭 노이즈를 방지할 수 있다.

CP 적용 과정을 그림 3에 나타냈다. 그림 3 (a)의 OFDM 심볼 양 끝단 강조한 부분이 CP 대상이다. 그림 3 (b) 양 단에 CP가 삽입된 모습을 보인다. CP1을 신호의 후미에 복사·배치하며, CP2를 신호의 선두에 복사·배치한다. 그림 3 (c)는 클릭 노이즈 방지를 위한 윈도우 함수를 나타낸다. 그림 3 (d)는 이 윈도우 함수가 적용된 통신 심볼을 보인다.

그림 4는 두 개의 OFDM 심볼이 접하는 구간에서의 스펙트로그램을 나타낸다. 그림 4 (a)는 윈도우 함수를 적용하지 않은 경우로, 심볼 접점에서 발생하는 클릭 노이즈에 의해 광대역 잡음 성분이 나타남을 확인할 수 있다. 반면, 그림 4 (b)는 윈도우 함수를 적용한 경우로, 동일 구간에서 광대역 잡음이 억제된 모습을 확인할 수 있다. 이러한 클릭 노이즈의 파워는 인접 샘플 간의 크기 차이에 따라 달라진다.

2. 수신기 구조

DQPSK 복조를 위해 수신 신호 $o'_k[n]$에 DFT 연산을 다음과 같이 수행한다.

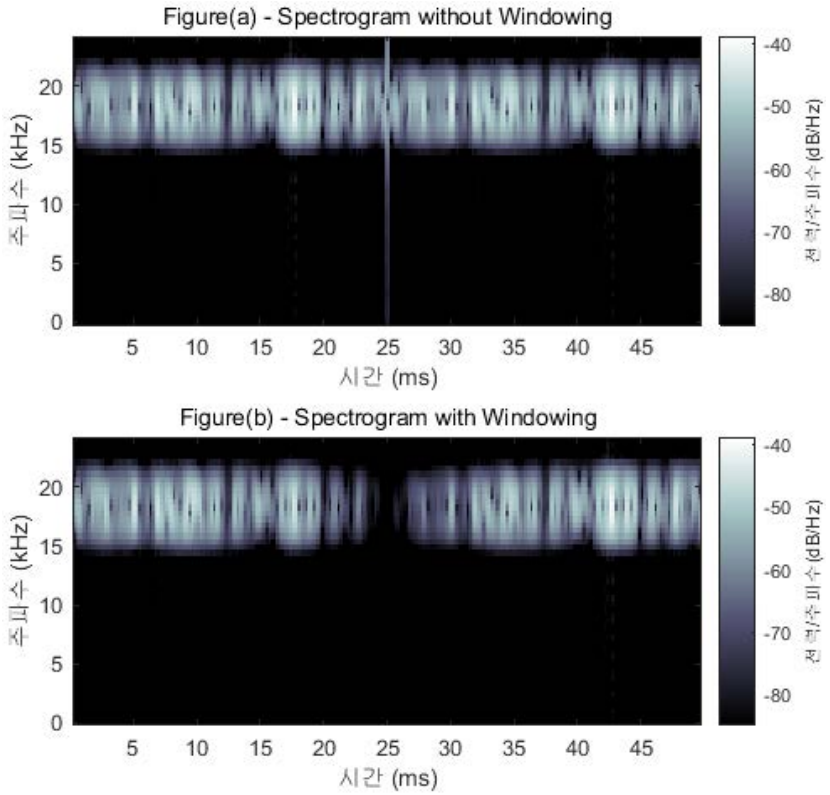

그림 4. (a) 윈도우 함수를 적용하지 않은 경우 스펙트로그램 (b) 윈도우 함수를 적용한 경우 스펙트로그램
Fig. 4. (a) Spectrogram without applying the window function (b) Spectrogram with the window function applied

$$O_k'[n] = DFT\{o'_k[n]\} \tag{11}$$

$O_k'[n]$는 OFDM 푸리에 윈도우로, 도플러 헤더 서브캐리어와 데이터 서브캐리어를 가지고 있다. 통신에 있어, 송신기 또는 수신기의 물리적인 이동으로 인해 도플러 효과가 나타나 통신 신호의 주파수가 천이하였을 수 있다. 이에 도플러 헤더 서브캐리어를 다음과 같이 탐색한다. 이는 도플러 헤더 서브캐리어의 기준 위치에서 $[k_l - n_{doppler}, k_l + n_{doppler}]$ 영역의 주파수 bin을 확인하여, 가장 큰 에너지의 위치를 찾는 방식으로 이뤄진다.

$$k_\delta = \left(\arg max_{\ k_l - n_{doppler} \le n \le k_l + n_{doppler}} |O'_k[n]|\right) - k_l \tag{12}$$

도플러 효과에 의해, OFDM 데이터 서브캐리어는 $[k_l + k_\delta + n_{doppler}, k_l + k_\delta + n_{doppler} + n_{subcarriers}]$ 영역에 나타난다. 앞서 송신기는 송신 데이터를 누산하여 각 데이터 서브캐리어에 할당하였다. 데이터 복조를 위해 먼저, OFDM 데이터 서브캐리어의 각 위상을 다음과 같이 차분 연산한다.

$$\begin{aligned} d'_k[n] = \ & [\theta\{O'_k[n + k_l + k_\delta + n_{doppler} + 1]\} - \\ & \theta\{O'_k[n + k_l + k_\delta + n_{doppler}]\}] \bmod 2\pi \end{aligned} \tag{13}$$

이어서 각 위상 차이에 따른 데이터 복조를 수행한다. 이는 다음과 같이 최소 유클리드 거리 추정 방식으로 각 심볼의 정보를 결정한다.

$$r'_k[n] = \begin{cases} 0\ (\frac{7}{4}\pi \le d'_k[n] < 2\pi) \\ 2\ (\frac{5}{4}\pi, \le d'_k[n] < \frac{7}{4}\pi) \\ 3\ (\frac{3}{4}\pi \le d'_k[n] < \frac{5}{4}\pi) \\ 1\ (\frac{1}{4}\pi, \le d'_k[n] < \frac{3}{4}\pi) \\ 0\ (0 \le d'_k[n] < \frac{1}{4}\pi) \end{cases} \tag{14}$$

식 (14)에 따른 결정 영역은 그림 5와 같다.

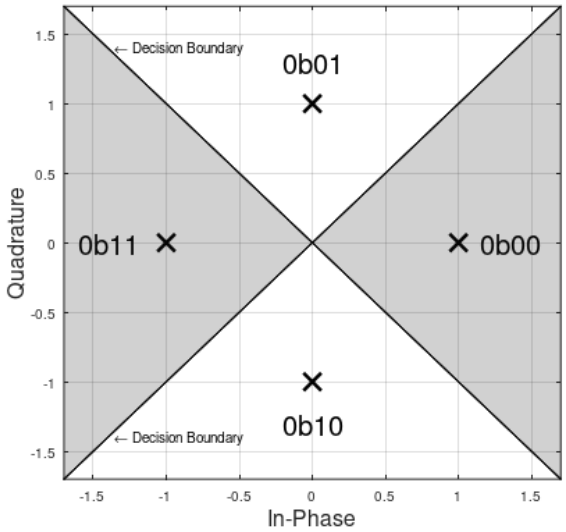

그림 5. 인접 서브캐리어 위상 차이의 비트 결정 영역
Fig. 5. Decision boundary using the phase difference of adjacent sub-carriers

Ⅳ. 음파통신 모뎀 구현

1. 안드로이드 스마트폰 화면 구성과 각 요소의 역할

그림 6에 음파통신 애플리케이션이 동작하는 실제 안드로이드 기기를 나타냈다.

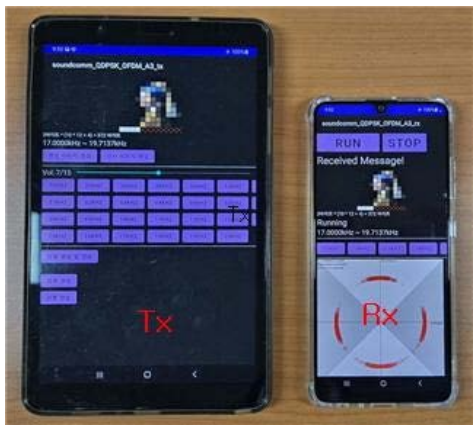

그림 6. 음파통신 안드로이드 애플리케이션 동작 모습
Fig. 6. Android implementation of acoustic communication

그림의 좌측이 송신기 앱의 모습이며 우측이 수신기 앱의 모습이다. 각 송신기와 수신기 앱 화면 구성은 다음과 같다.

송신기는 앱 화면의 상단부터 차례대로 다음의 기능을 가진다.

1) 데이터 표시: 통신의 목적이 되는 데이터를 이미지로 보인다.
2) 기본 동작 정보 표시: 통신이 이뤄지는 주파수 대역과 데이터 정보량 크기를 보인다.
3) 데이터 변경: 통신 데이터를 다양하게 바꿀 수 있다.
4) 기기 볼륨 설정: 하드웨어의 음량을 보이며, 이를 조절할 수 있다.
5) 통신 대역 지정: 통신 대역 하단 주파수를 바꿀 수 있다. 단, 대역폭은 항상 2.71 kHz로 동일하다.
6) 신호 재생: 통신 신호를 생성하거나 재생할 수 있다. 한번 생성된 신호는 메모리에 저장되므로, 반복 재생할 수 있다.

수신기는 앱 화면의 상단부터 차례대로 다음의 기능을 가진다.

1) 동작 설정: 통신 기능을 켜고 끌 수 있는 기능이다.
2) 현재 상태: 통신 기능의 상태를 보인다. 처프 신호 감지 내지는 통신 성공이나 통신 실패 상황을 보인다.
3) 통신 데이터: 통신이 성공할 경우, 수신 데이터를 이미지로 나타내 보인다.
4) 기본 동작 정보 표시: 통신이 이뤄지는 주파수 대역과 데이터 정보량 크기, 그리고 동작 상태를 보인다.
5) 통신 대역 지정: 통신 대역을 바꿀 수 있다. 송신기와 동일한 지정 값이어야만 통신이 이뤄질 수 있다.
6) 성상도: DQPSK에 따른 서브캐리어의 위상차를 보인다. 앱 동작에 있어, 성능 최적화를 위해 인접 서브캐리어의 위상차만 계산한다. 이에 크기가 1로 정규화된 성상도를 보인다.

2. 통신 데이터 구성

이 논문에서 보이는 통신 시스템은 372 바이트의 데이터를 송·수신한다. 372 바이트 데이터는 영문 372자 또는 한글 186자를 표현할 수 있는 크기로, 이를 한 화면에 표현하기에는 많은 양의 데이터이다. 반면, 이미지는 한 픽셀당 3 바이트 (RGB 채널)로 구성되어 전체 데이터를 124개의 픽셀에 표현할 수 있어, 대용량 데이터를 시각적으로 나타내기에 적합하다. 전체 데이터는 다음과 같이 각 픽셀에 대입된다.

$$[R_0, G_0, B_0, R_1, G_1, B_1, R_2, G_2, B_2, \ldots, R_{123}, G_{123}, B_{123},] \quad (15)$$

예를 들어, 통신 데이터가 [0x32, 0x3F, 0x6C, 0x77, 0x86, 0x7B, 0x2E, 0x3A, 0x68, 0x35, 0x45, 0x77 ...]일 경우, 1) 첫 번째 픽셀은 [R = 0x32, G = 0x3F, B = 0x6C]이며, 2) 두 번째 픽셀은 [R = 0x77, G = 0x86, B = 0x7B]이다.

이를 그림 7에 나타냈다.

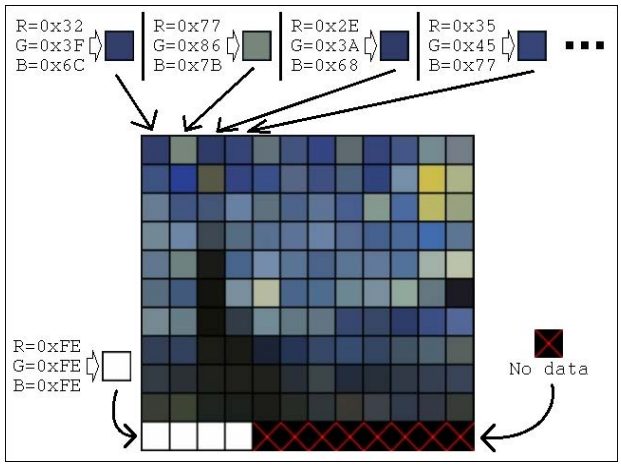

그림 7. 송·수신 데이터 자료 표현 방법
Fig. 7. Data representation format

3. RSA 암호 적용

RSA 암호화된 메시지를 송·수신하기 위해 Java의 java.security 패키지를 이용하였다[11]. 이 Java Security API는 Java Development Kit (JDK)에 포함된 것으로, KeyFactory, KeyPair, PublicKey, PrivateKey 등의 하위 API를 제공하여 RSA 암호화·복호화 기능을 간단하게 적용할 수 있도록 한다. 이를 이용하여 PKCS #1 v2.2 표준의 RSA 암호를 적용하였다. 이 표준에 따르면 RSA 모듈로 바이트

길이 k에 대해, 메시지의 길이는 최대 k-11 바이트가 될 수 있다[8]. 즉, PKCS #1 v2.2 표준에서 평문은 최대 245바이트이다[13].

그림 8에 RSA 암호를 적용한 통신 앱을 보였다. 그림의 좌측이 수신기이며, 우측이 송신기이다. 평문 245 바이트를 이미지로 표현하되, 나머지 2 바이트를 이미지 우측에 16진법 숫자로 나타냈다. 송신기는 PKCS #8 표준의 포맷으로 표현된 모듈로 N의 정보를 화면에 보이고 있으며, 10진수 65,537에 해당하는 0x010001 공개 키를 화면에 보인다. 수신기는 PKCS #8 표준의 포맷으로 구성된 개인 키를 화면에 보인다. 송신기의 모듈로 N 정보는 총 257 바이트이며, 수신기의 개인 키는 전체 1,217 바이트에 달해, 화면에 자료의 첫 일부만 표시하였다.

그림 8. RSA-2048 비대칭 키 암호문 송·수신 모습
Fig. 8. RSA-2048 asymmetric key transmission

Ⅴ. 성능평가

이 시뮬레이션은 통신 신호에 AWGN 신호가 가해졌을 때의 통신 성능을 확인하기 위해 실시하였다. 시뮬레이션을 통해, SNR에 따른 DQPSK의 심볼 오류율 SER을 확인할 수 있다. MATLAB의 randn 함수를 이용해 AWGN 채널 환경을 구성하였다. 단, 이 함수를 이용해 생성한 노이즈 신호는 통신 대역 이외의 주파수에도 에너지를 고르게 가지고 있다. 이에 대역 내 SNR은 다음과 같이 정의된다.

$$\text{In band } SNR = 10\log_{10}\left(\frac{\sum_{i=1}^{5n_{symbol}} s[i]^2}{\frac{f_h - f_l}{f_s/2} \times \sum_{i=1}^{5n_{symbol}} n[i]^2}\right) \quad (16)$$

전체 대역폭 24,000 Hz 대비 실제 통신 대역폭의 비율만큼 노이즈 에너지에 곱셈함으로써 대역 내 SNR를 구하였다. 시뮬레이션 모의 채널 신호는 AWGN 신호의 무작위 위치에 통신 신호를 배치한 모습이다. 시뮬레이션은 수신기의 실제 동작과 동일한 블록 연산을 수행한다. 시뮬레이션은 이 모의 채널 신호를 n_{symbol} 샘플만큼 나누어 모의 수신기에 차례로 입력함으로써 진행된다. 이에 모의 수신기는 처프 신호를 감지, DQPSK 복조와 RS 오류 정정에 이르기까지 모든 과정을 수행한다.

시뮬레이션 환경에서 모의 수신기는 통신 메시지를 송신 원본 메시지와 비교할 수 있도록 하였다. 이를 통해 DQPSK 심볼 오류율을 기록할 수 있다. DQPSK 심볼 오류율은 전체 5,120개의 DQPSK 심볼 가운데, 송신 원본 메시지와 다른 DQPSK 심볼의 비율을 나타낸다. 심볼 길이 n_{symbol}의 변화에 따른 통신 성능 변화 확인을 위해 $n_{symbol} = 12{,}000$과 $n_{symbol} = 48{,}000$ 환경에서 또한 시뮬레이션을 수행하였다. 0 dB에서 25 dB까지 0.5 dB 간격의 SNR 환경에서, $n_{symbol} = 12{,}000$에서 20,000회 반복 실험하였으며, $n_{symbol} = 24{,}000$에서 100,000회 반복 실험하였으며, $n_{symbol} = 48{,}000$에서 20,000회 반복 실험하였다.

컴퓨터 시뮬레이션 결과와 나란히 비교하기 위해 무향실 환경에서 실제 기기를 이용한 실험을 진행하였다. 실제 실험은 0 dB에서 15 dB까지 1 dB 간격의 SNR 환경에서 진행하였으며, $n_{symbol} = 24{,}000$에서 100회 반복 실험하였다. 통신 신호는 시뮬레이션에서의 신호를 이용하였다. 송신 장치와 수신 장치는 사전에 약속된 메시지를 주고받도록 실험을 구성하였다. 이에 수신 장치는 통신 메시지에 대해 DQPSK 심볼 오류율과 통신 성공률을 확인할 수 있다. 실제 실험 환경을 표 2에 정리하였다. 또한 위 실험 환경에 따른, SNR에 따른 DQPSK 심볼 오류율은 그림 9에 나타냈다. SNR은 신호의 전력/잡음의 전력이기 때문에 시간을

표 2. 휴대폰을 이용한 실험의 환경
Table 2. Parameters for test

Test Environments		Value
Hardware	Receiver	Samsung Galaxy A32 (SM-A325N)
	Transmission Speaker	ADAM Audio A3X
	Signal Generator	Audio Precision APx517B
	Microphone for Noise Measurement	GRAS 46AE
Signals	Bandwidth	17,000 Hz ~ 19,713 Hz
	Signal Duration	2,500 ms
	Transmission Period	9 seconds
	Sampling Frequency	48,000 Hz
Chamber	Tx Rx Distance	1 m
	Chamber Temperature	22.3 ℃
	Chamber Noise	39.1 dBA
	Chamber Size	1,400 mm × 600 mm × 600 mm (L×W×H)

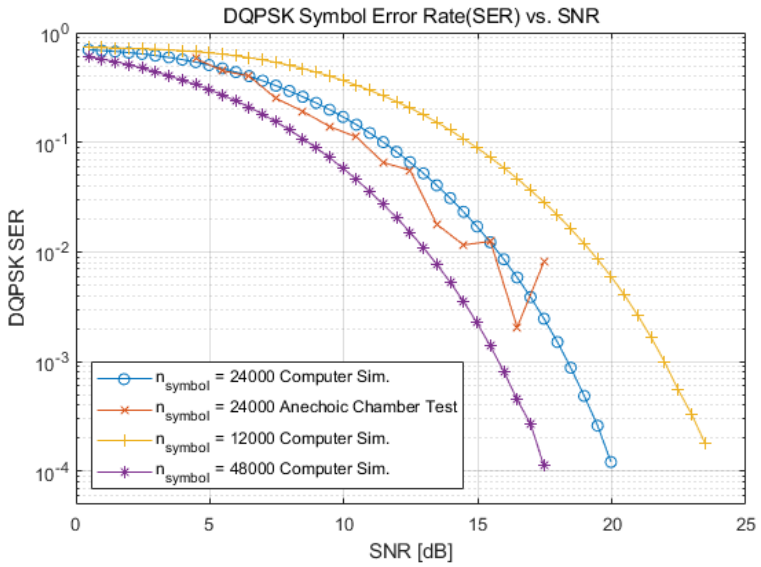

그림 9. SNR에 따른 음파통신 OFDM DQPSK의 심볼 오류율
Fig. 9. Symbol error rate of DQPSK OFDM Acoustic communication system

길게 하여 전송하는 경우 비트 당의 에너지가 커지면서 성능이 좋아지는 것을 확인할 수 있다. 또한 측정값과 시뮬레이션 결과가 거의 일치하는 것 또한 확인할 수 있다.

Ⅵ. 결 론

이 논문에서 OFDM 기반 DQPSK를 이용한 음파통신을 보였다. 통신 신호는 17 kHz에서 19.71 kHz의 음파 가청 주파수 대역을 이용하며, 시간 영역에서 전체 2.5초 길이를 가진다. 한 번의 신호 발생으로 송신기는 최대 372 바이트에 이르는 데이터를 송신할 수 있다. 이는 2,048 비트 키를 가지는 비대칭 키 암호 시스템 RSA의 256 바이트 암호문 메시지를 성공적으로 보낼 수 있다.

안드로이드 스튜디오 개발 도구를 이용해 실제 통신 시스템 애플리케이션을 구현하였으며, 이를 이용해 시뮬레이

션 결과와 같이 동작 성능을 확인하였다. 이 통신 시스템은 비대칭 키 암호를 적용한 통신으로써, 근거리에서 금융 결제에 필요한 정보나, 각종 비밀번호 또는 기타 중요 정보를 송·수신하는데 적용할 수 있을 것으로 기대된다.

참 고 문 헌 (References)

[1] S. Lin and D. Costello, *Error Control Coding*, 2nd Edition, Pearson, 2004.
doi: https://dl.acm.org/doi/book/10.5555/983680

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 3rd Edition, Chapman and Hall/CRC, 2025. https://www.cs.umd.edu/~jkatz/imc.html

[3] Y. Hornych, J. C. Toledo, B. Wang, W. -J. Yi and J. Saniie, "Near-Ultrasonic Communications for IoT Applications using Android Smartphone," 2020 *IEEE International Conference on Electro Information Technology* (EIT), Chicago, IL, USA, 2020. https://ecasp.ece.iit.edu/publications/2012-present/2020-10.pdf

[4] H. Lee, T. H. Kim, J. W. Choi and S. Choi, "Chirp signal-based aerial acoustic communication for smart devices," 2015 *IEEE Conference on Computer Communications* (INFOCOM), Hong Kong, China, 2015. https://snu.elsevierpure.com/en/publications/chirp-signal-based-aerial-acoustic-communication-for-smart-device/

[5] H. Matsuoka, Y. Nakashima, and T. Yoshimura, "Acoustic comunication system using mobile terminal microphones," *NTT DoCoMo Tech. J.*, vol.8, no. 2, pp. 2 – 12, 2006. https://api.semanticscholar.org/CorpusID:53339203

[6] P. Getreuer, C. Gnegy, R. F. Lyon and R. A. Saurous, "Ultrasonic Communication Using Consumer Hardware," *IEEE Transactions on Multimedia*, vol. 20, no. 6, pp. 1277-1290, June 2018.
doi: https://doi.org/10.1109/TMM.2017.2766049

[7] H. Fletcher and W. A. Munson, "Loudness, its definition, measurement and calculation," *Journal of the Acoustical Society of America*, vol. 5, pp. 82 – 108, 1933.
doi: https://doi.org/10.1002/j.1538-7305.1933.tb00403.x

[8] "AudioFormat - sampleRate," Android Developers, [Online]. Available: https://developer.android.com/reference/android/media/AudioFormat#sampleRate. [Accessed: Dec. 4, 2024].

[9] Y. S. Cho, J. Kim, W. Y. Yang, and C. J. Kang, *MIMO-OFDM Wireless Communications with MATLAB*, Wiley-IEEE Press, 2010. https://ieeexplore.ieee.org/book/5675894

[10] J. Proakis and M. Salehi, *Digital Communications*, 5th Edition, McGraw-Hill Education, 2007. https://www.amazon.com/Digital-Communications-5th-John-Proakis/dp/0072957166

[11] "JavaTM Cryptography Architecture (JCA) Reference Guide," [Online]. Available: https://developer.android.com/reference/java/security/ package-summary

[12] J. M. Snell and F. R. Moore, *Elements of Computer Music*, Leonardo Music Journal, p. 157, 1990. https://www.researchgate.net/publication/271081534_Elements_of_Computer_Music

[13] B. Kaliski and J. Staddon, "PKCS #1: RSA Cryptography Specifications Version 2.2," RFC 8017, Internet Engineering Task Force, Nov. 2016. [Online]. Available: https://datatracker.ietf.org/doc/rfc8017/

저 자 소 개

박 찬 휘

- 서울시립대 전자전기컴퓨터공학과 학석사
- 현재 : 삼성전자 모바일사업부 연구원
- ORCID : https://orcid.org/0009-0006-4550-8491
- 주관심분야 : 무선통신, 디지털 오디오 신호처리

김 영 길

- 현재 : 서울시립대 전자전기컴퓨터공학부 교수
- ORCID : https://orcid.org/0000-0001-7066-0555
- 주관심분야 : 무선통신, 디지털 오디오 신호처리