UNIVERSITY OF CALIFORNIA SAN DIEGO

Power Efficient RF Transceiver Design Using 16-FSK Modulation

A dissertation submitted in partial satisfaction of the
requirements for the degree Doctor of Philosophy

in

Electrical Engineering (Electronic Circuits and Systems)

by

Ali Nikoofard

Committee in charge:

Professor Patrick P. Mercier, Chair
Professor Gert Cauwenberghs
Professor Prasad Gudem
Professor Drew Hall
Professor Laurence B. Milstein

2021

The Dissertation of Ali Nikoofard is approved, and it is acceptable in quality and form for publication on microfilm and electronically.

University of California San Diego

2021

DEDICATION

To myself, my family and all that helped me within this journey.

EPIGRAPH

You do not understand anything unless,
you learn in more than one way.

Marvin Minsky

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

As My journey as an electrical engineer started from 2008 till now, the basis for my dissertation research originally stemmed from my passion to use more than a decade experience of academic back ground plus the enthusiasm toward introducing innovative circuit that can offer a solution for existing radio communication problems.

The motivation behind this work rises from the fact that as in modern era, the need for systems that are utilized for high speed, high performance, and low power radio application is at its highest, it requires new and more efficient IC solutions.

In this dissertation, multiple design techniques and innovative circuits are introduced that by offering novel approaches introduce acceptable solution for long-range low power radio communication. Multiple test chips have been fabricated and been measured to demonstrate the functionality of the proposed IC solutions.

In truth, I could not have achieved my goal, but with sacrifices made by me, team mates and supervisors within the times to establish an smooth path for success.

ACKNOWLEDGEMENTS

I would like to acknowledge Professor Patrick P. Mercier for his support as the chair of my committee. Through multiple drafts and many long nights, his guidance has proved to be invaluable.

I would also like to acknowledge the "Hamed Abbasi-Zadeh" of EEMS lab, without whom my research would have no doubt taken fives times as long. It is their support that helped me in an immeasurable way.

Chapter 1, in full, is a reprint of the material as it appears in Journal of Solid-State Circuits, 2021, Nikoofard, Ali; Abbasi-Zadeh, Hamed; Mercier, Patrick P., IEEE Press, 2021 and the material as it appears in 2020 Symposium of VLSI Circuits 2020, pp. 1-2, Nikoofard, Ali;Abbasi-Zadeh, Hamed; Mercier, Patrick P., IEEE Press, 2020. The dissertation author was the primary investigator and author of this paper. I would like to acknowledge "Hamed Abbasi-Zadeh" of EEMS lab as the second author of the work and all his help during the measurement.

Chapter 2, in part is currently being prepared for submission for publication of the material. Nikoofard, Ali; Mercier, Patrick P. The dissertation author was the primary investigator and author of this material.

Chapter 3, in part is currently being prepared for submission for publication of the material. Nikoofard, Ali; Mercier, Patrick P. The dissertation author was the primary investigator and author of this material.

VITA

2012–2015 Master of Science, in Micro-Electronics, Sharif University of Technology, Tehran

2015–2017 Master of Science, in Electrical Engineering and Computer Science, Case Western reserve University, Cleveland

2017–2021 Doctor of Philosophy, in Electrical Engineering (Electronic Circuits and Systems), University of California San Diego

2018–2021 IC Design Engineer, MaXentric Technologies LLC, La Jolla

PUBLICATIONS

"A 0.6-mW 16-FSK Receiver Achieving a Sensitivity of -103 dBm at 100 kb/s," in IEEE Journal of Solid-State Circuits, vol. 56, no. 4, pp. 1299-1309, April 2021.
"A 920MHz 16-FSK Receiver Achieving a Sensitivity of -103dBm at 0.6mW Via an Integrated N-Path Filter Bank," in 2020 IEEE Symposium on VLSI Circuits.
"A -254.1-dB FoM 2.4-GHz Subsampling PLL With a -76-dBc Reference Spur by Employing a Varactor-Based Cancellation Technique," in IEEE Solid-State Circuits Letters, vol. 3, pp. 102-105, 2020.
"A 0.3-V CMOS Biofuel-Cell-Powered Wireless Glucose/Lactate Biosensing System," in IEEE Journal of Solid-State Circuits, vol. 53, no. 11, pp. 3126-3139, Nov. 2018.
"A 0.3V biofuel-cell-powered glucose/lactate biosensing system employing a 180nW 64dB SNR passive ΣΔ ADC and a 920MHz wireless transmitter," in 2018 IEEE International Solid - State Circuits Conference - (ISSCC), 2018, pp. 284-286.

FIELDS OF STUDY

Major Field: Electrical Engineering (Radio Frequency Integrated Circuit)

Studies in Phased Locked Loops

Studies in M-ary FSK Optimum Demodulator

ABSTRACT OF THE DISSERTATION

Power Efficient RF Transceiver Design Using 16-FSK Modulation

by

Ali Nikoofard

Doctor of Philosophy in Electrical Engineering (Electronic Circuits and Systems)

University of California San Diego, 2021

Professor Patrick P. Mercier, Chair

The demand for higher performance radio communication increases every day. Since the radio spectrum is highly occupied, modern radio systems require to maximize the data rate, through put, and minimize the cost of that radio, its noise and power consumption. Within the given scenario, there are two major factors, the first is spectrum efficiency (SE) and the second one is power efficiency (PE). Former is related to maximum data rate within the given spectrum limit and the latter is addresses by the required E_b/N_0 (energy per bit over noise power spectral density) to demodulate the input signal with acceptable error rate. In many radio applications, due to stationary nature of the radio system, PE can be compromised. However, in application that include the mobile battery in the system, PE must be optimized to the maximum extent to

increase the lifetime of the system.

Applications that require long range communication while having a mobile battery systems appear crucial to have high PE with acceptable signal fidelity. We have explored a known M-ary FSK modulation and shown that using the modulation optimally, there can be notable improvement in the system PE. Therefore multiple test chips have been fabricated to show the feasibility of enhanced PE in M-ary FSK transceivers.

Introduction

Handheld wireless radio systems that require to operate over long range (km range) requires large batteries within the system. This by nature, makes those system less desirable since the users need to carry heavy batteries. The reason that systems as such require to increase their power consumption is directly related to the free space path loss that will cause the input signal delivered from one communication node to another be very small (nano Watt range in power, and also assuming small fading effects). The main communication parameter within the given data rate is usually identified by the receiver sensitivity which is a function of received signal/noise bandwidth, required signal to noise ratio for the demodulator and the overall receiver noise figure. Since, we have identified the system that currently exist are not suitable for users of such applications, such as soldiers inside of the field that would need to carry small radio systems, in this dissertation, we have tackled this issue by introducing a receiver that is very small, light and consume small power (less than 1mW) and achieves the required performance with the test Silicon integrated circuit.

Within the given link budget of receiving nano Watt RF energy at the antenna, and having the total receiver power consumption below than 1 mW, Fig. 1 shows that recent works are closing the gap to offer the solution, however still there exist no system that can optimally solve the problem [WAI20b].

As it can be seen from Fig. 1, for all radios and also standard compatible radios, there are hand-full of the design that have achieved below -100 dBm sensitivity and most of the few that have achieved such a performance, consume the power more than 1 mW. The importance of the sensitivity mostly shows it self by knowing that free space path loss with 10 dB margin would be

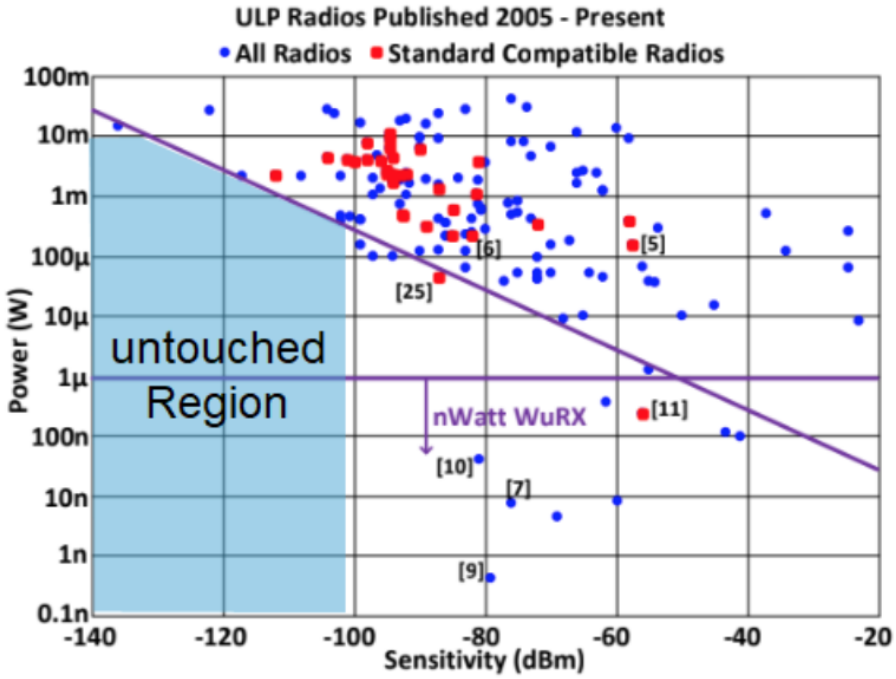

Figure 1. Ultra low power receivers survey, courtesy of David Wentzloff [WAI20b].

cause around 100 dB loss. Also, assuming the transmitter power is confined by mW range, with 0 dBm radiation, the sensitivity levels of -100 and below would be more eminent. Therefore, the target for this work was set to design a receiver that lie within the untouched region shown in Fig. 1 by introducing new circuit and system solutions. The summary of the problem and possible integrated solution while for instance, in this case, soldiers are in the field and there are point to point radio communication alongside with the free space path loss is depicted in Fig. 2.

In this dissertation, methods of improving the receiver sensitivity by taking advantage of inherent power efficiency improvement of M-ary FSK modulation is fully studied and a test chip has been fabricated for the proof of concept. Since the proposed power efficient technique can also be used for the transmitter, a direct modulation technique for the transmitter side is studied and implemented with the test chip measurement. The complete transceiver solution for the long range low power communication has been completed within the dissertation.

Furthermore, we have also studied the short range low power communication, but with

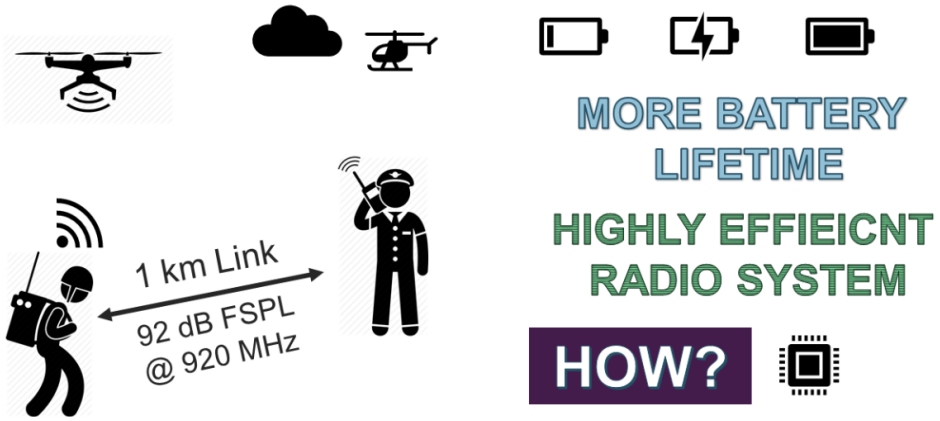

Figure 2. Existing problem for long range low power radio communication.

the focus of improving the overall system privacy. Recognizing the challenge in standards that are widely and daily used such as Bluetooth Low Energy (BLE)/ WiFi and offering a solution to an existing problem that has not yet been addressed by literature is of great importance. Fingerprinting radio signal features in I/Q modulators which is the typical structure for the aforementioned standards, opens the door for adversaries to identify and locate the users. In this dissertation, we have proposed a robust and effective technique in which standards such as BLE and WiFi can take of take advantage of that, and without losing the signal fidelity, increase the communication privacy by randomizing the features that would confuse any adversary and decrease the confidence of the recognition. Overall, in this dissertation, innovative low power circuits and communication techniques have come together to solve the existing long range low power light-system radio communication problems along side privacy enhancement of short range communication. The author encourages the respected readers to study this dissertation with detail along side the published papers.

The rest of the dissertation has been divided in three chapters accordingly. Chapter. 1 presents a low power receiver in which utilizes a high efficiency modulation, 16-FSK (frequency shift keying) to enhance the PE while maintain low power operation using innovative circuits.

Chapter. 2 studies the implementation of the 16-FSK direct conversion transmitter with highly efficient single-transistor power amplifier.

Chapter. 3, last but not least, introduces an approach for highly ambivalent BLE/WiFi using devices that can considerably solve their privacy concern and enhance the user identity safety by randomizing the transmitted signal features, while not affecting the signal fidelity.

Fig. 3 demonstrates the integrated circuits designed for each project by dissertation author as the primary investigator, respectively from top to bottom. All the test chips are fabricated in 65nm LPCMOS technology node. Measurements across different sample in each chapter shows the performance of the proposed IC solution.

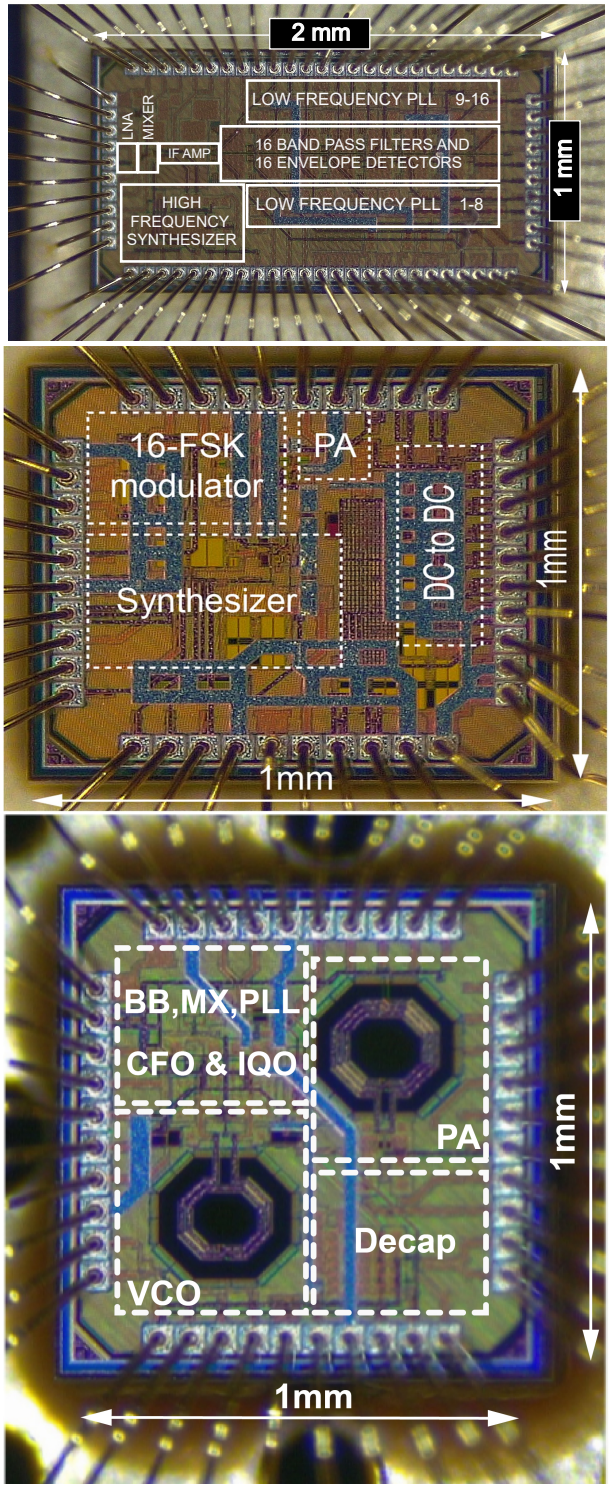

Figure 3. Chip Gallery - Low Power 16-FSK Receiver, Low Power 16-FSK Transmitter, and Enhanced Privacy WiFi/BLE Transmitter, from top to bottom, respectively.

Chapter 1

Low Power 16-FSK Receiver

1.1 Abstract

This chapter presents an RF receiver designed to exploit the inherent SNR advantage offered by non-coherent 16-FSK modulation relative to more conventional non-coherent modulation schemes such as FSK and OOK. Specifically, the design demonstrates that, when demodulated using two-pole band pass filters, 16-FSK offers a 4 dB sensitivity advantage compared to BFSK, at the cost of reduced spectral efficiency at the same data rate. The chapter then presents the design of a 16-FSK-compatible receiver front-end, which performs demodulation through 16 N-path filters driven by temperature-stabilized phase locked loops to ensure calibration-free filter center frequency control, along with augmented Miller capacitors for tight area-constrained bandwidth control. Implemented in 65 nm CMOS, the receiver consumes 0.6 mW from a 0.5 V supply, while achieving a sensitivity of -103.2 dBm at 100 kbps, for a power-sensitivity-data-rate figure of merit of 185.2 dB, which represents a 3.2 dB advance over state-of-the-art.

1.2 Introduction

Distributed wireless sensor networks, particularly those operating in areas where no existing wireless infrastructure exist, have unique power-related challenges not typically encountered in conventional radio design. For example, most low-power radio communication systems exploit the inherent energy asymmetry in networks organized with a star topology: the

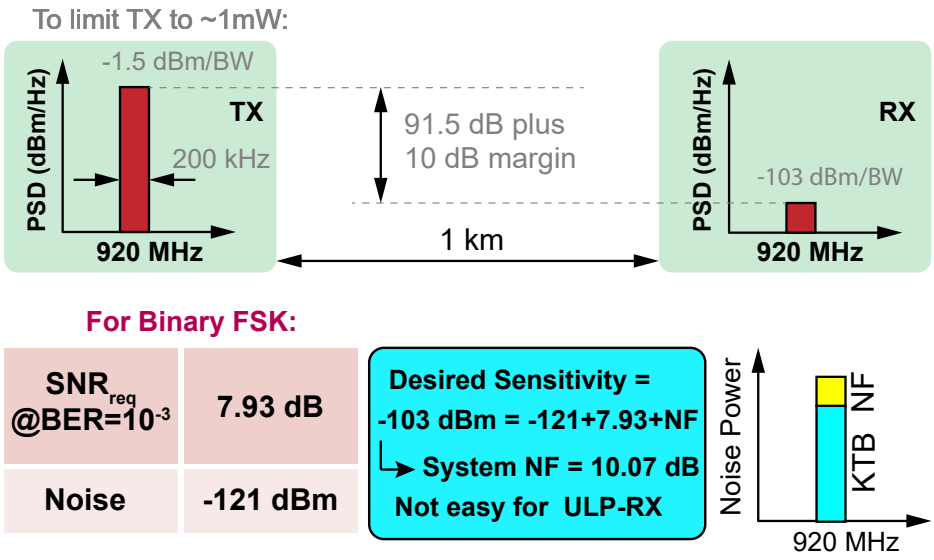

Figure 1.1. Link budget calculation of a long range, low-power BFSK system.

energy-rich base-station can help overcome the weaknesses of energy-starved individual nodes by, for example, generating additional transmitter (TX) output power to overcome poor receiver (RX) sensitivity on the energy-starved node. However, many emerging classes of Internet of Things (IoT) applications such as smart agriculture, perimeter monitoring, weather stations, etc. can reach across many kilometers of distance, and building centralized towers to operate as base-stations across these distances can be prohibitively costly.

An alternative approach is to create an ad-hoc mesh network, where each individual node communicates information to its neighbor. Unlike star topologies, such mesh-based topologies cannot typically exploit energy asymmetry: all devices in the network are energy constrained, as they are typically powered by small batteries or energy harvesters. Consequently, radios embedded into mesh networking nodes must ideally be efficient in both the TX mode and the RX mode to maximize battery lifetime. This requires a different type of link and radio optimization strategy than is typically employed in energy-asymmetric networks.

Fig. 1.1 outlines the link budget requirements of an example system where both TX and RX are restricted to $\sim$1 mW of power consumption, and yet must communicate over a $\sim$1 km link with a data rate of 100 kbps. In a star network with an energy-unconstrained base-station,

this is trivial to achieve: a $+30$ dBm TX output, even after 1 km of path loss at 920 MHz (91.5 dB) plus 10 dB of margin, requires -71.5 dBm of receiver sensitivity, which is easily achievable at sub-mW power levels [PGR08, PSO11, SLP14]. However, when TX output power is restricted to sub-mW levels (to account for the efficiency of the power amplifier and the power of downstream components), the required RX sensitivity drops to -103 dBm, which, as will be seen in Section 1.3 , is difficult to achieve at low-power and at 100 kbps (note: a more detailed link budget description will be given in Link Budget Section.

The chapter is organized as follows. Section 1.3 begins by first reviewing popular low-power design techniques and associated state-of-the-art designs. Section 1.4 then discusses link budgeting in detail, including a discussion of how the 16-FSK modulation scheme enables relaxed specifications towards achieving the desired link budget. Section 1.5 describes the proposed receiver architecture, including a discussion of how to build a near-optimal, yet robust and low-power 16-FSK demodulator. Section 1.6 then presents measurement results from the fabricated chip, and Section 1.7 concludes the chapter.

1.3 Overview of Low-Power Receiver Architectures

In the pursuit of reducing power consumption, most work in the low-power radio literature utilizes low-order modulation schemes with non-coherent reception such as on-off keying (OOK) or binary frequency shift keying (BFSK) [Mer15, WAI20a]. Since phase does not need to be tracked, non-coherent demodulation of such modulation schemes has the major advantage of not requiring a precise local oscillator (LO). Since precision phase locked loops (PLLs) with low phase noise typically consume nearly all or in many cases more than the mW power budget [SMS18, LDNK18, KM20, LNM20], this can provide significant power savings.

In the extreme limit of non-coherent reception of OOK signals, no PLL at all is required, and instead the incident RF signal can be passively filtered directly at RF, followed by energy detection. While this technique has been used successfully for wake-up receivers that

consume nW power levels [WJG+18, MK19, MDB+19, JWG+20], the lack of filtering at the individual channel level, lack of filter programmability, and wide RF noise bandwidth make such architectures only suited for applications with very relaxed data rate and interference tolerance requirements. Taking this approach up to higher data rates typically results in deteriorated sensitivity [RCS+16].

Instead of relying purely on passive RF filtering, most low-power receivers operating at higher data rates and low sensitivities use an LO to mix the RF signal down to an intermediate frequency (IF), such that channel-select filtering can be accomplished more easily via the heterodyne approach. However, the lowest power receivers that utilize an LO tend to forgo the use of a PLL, and instead run the LO open loop [NPMC12, PGR08, APC18, IKW19]. While this indeed saves power, the uncertainty of the LO frequency means that either the IF will be uncertain, thereby necessitating a large IF bandwidth prior to energy-detection, which ultimately deteriorates the achievable sensitivity and eliminates the ability to distinguish channels with fine resolution, or frequent calibration is required, particularly if multi-channel operation is desired. For this reason, many designs end up using a low-power PLL for LO stabilization and/or channel selection capabilities [vvv+09, AMS+14, SJDL17, KJC+19, WM20].

Since much prior-art does not necessarily aim for the same data rate or power level as the current work, it can be difficult to directly compare between designs. To ease this comparison, the following figure of merit, which takes into account fundamental trade-offs between power consumption, data rate, and sensitivity, can be employed:

$$FoM = \text{-Sensitivity} + 10\log(\text{Data Rate}) - 10\log(\text{Power}). \tag{1.1}$$

For the desired specifications, namely a data rate of 100 kbps, a sensitivity of at least -103 dBm, and a power consumption less than 1 mW, a figure of merit of greater than 183 dB is required. Assuming an ideal demodulator, this corresponds to a total receiver noise figure of 10 dB or less for BFSK, as described in detail in Section 1.4.

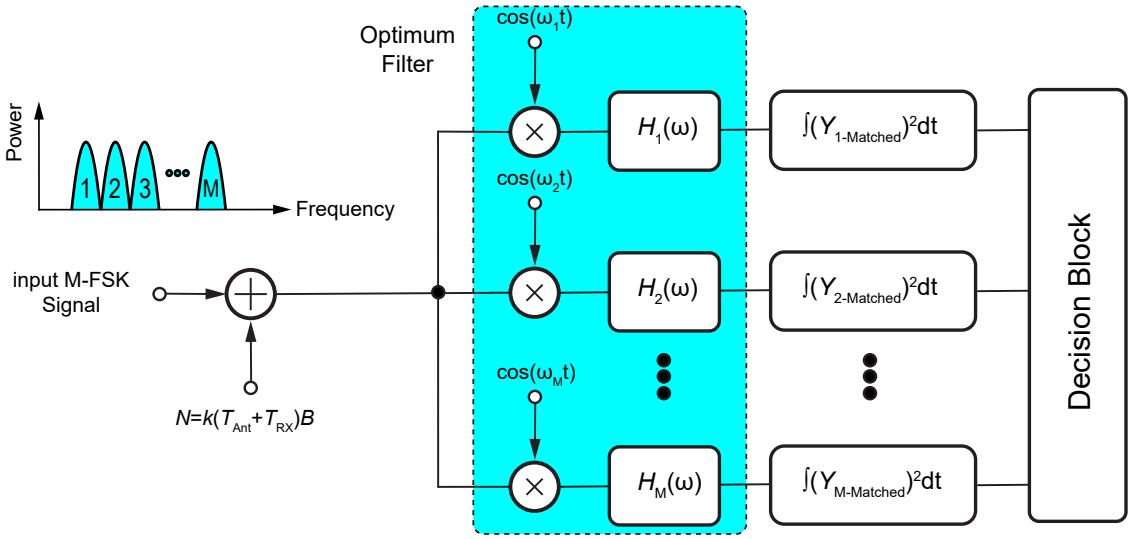

Figure 1.2. Optimal receiver structure for M-ary FSK.

Unfortunately, no prior art literature operating at data rates greater than 10 kbps meet these metrics. As an example, [WM20] utilized a sliding-IF-based architecture to reduce the required LO frequency; the resulting PLL consumed 322 μW, which is substantially lower than most PLLs used in coherent receivers, though in that design was 69% of the total RX power consumption of 455 μW. The design achieved a sensitivity of -102 dBm at a data rate of 25 kbps, for a resulting FoM of 179 dB. Assuming ideal matched filtering for FSK demodulation, the calculated noise figure was 17 dB. In [KJC+19], which coincidentally operated at the same carrier frequency and data rate as the proposed work (though with a much larger FSK frequency deviation), the authors employed a direct-conversion approach with a passive poly-phase-filter-based frequency-to-voltage demodulator. The employed PLL+VCO consumed 237 μW, or 47% of the total 499 μW power consumption. The received achieved a sensitivity of -99 dBm at 100 kbps, for an FoM of 182 dB. Although it's not clear how near to ideal the employed demodulator was, generously assuming it was near an ideal matched filter, the calculated noise figure of the design was 14 dB.

Thus, while the latest art is close to the desired specifications, further improvements are still necessary, especially if more margin is desired.

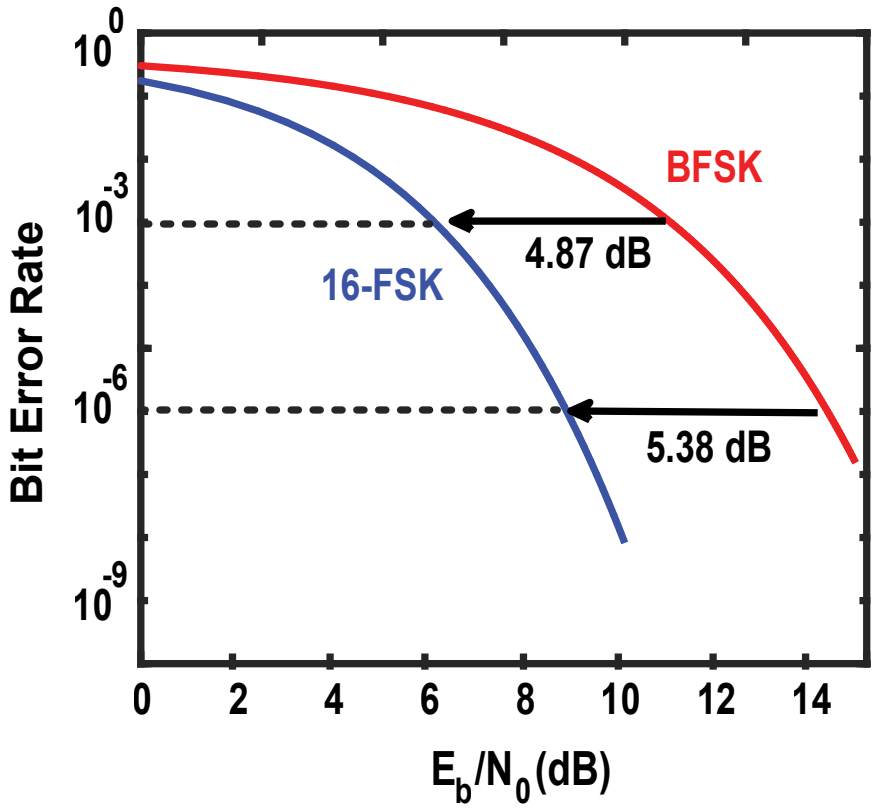

Figure 1.3. Bit error rate waterfall curves for BFSK and 16-FSK in an AWGN channel.

1.4 Analysis of the Link Budget

Assuming a total power consumption of 1 mW at both the TX and RX nodes imposes a strict link budget when operating over 1 km. Assuming a (generous) power amplifier efficiency of $\sim$70%, a maximum TX output power of -1.5 dBm is achievable. The power received at the receiver can be computed via the Friis transmission formula:

$$P_{RX} = P_{TX} + D_{TX} + D_{RX} + 20\log_{10}\left(\frac{\lambda}{4\pi d}\right), \tag{1.2}$$

where P_{RX} and P_{TX} are the receive and transmit power in dBm respectively, D_{RX} and D_{TX} are receive and transmit antenna directivities in dB, λ is the wave length in meters, and d is the distance between the transmitter and receiver node in meters. Replacing $P_{TX} = -1.5$ dBm, $d = 1$ km, and 0 dB directivity for both transmit and receive antenna at 920 MHz, the received

power will be -93 dBm. To account for adverse effects due to antenna shading, multi path fading, and so on, an additional 10 dB margin is typically included, bringing the required receiver sensitivity to -103 dBm.

The sensitivity of a receiver can be computed via the following equation:

$$\begin{aligned} P_{\text{sensitivity}} &= kTB \times NF \times SNR \ \text{ [linear]} \\ &= -174 \text{ dBm/Hz} + 10\log_{10}(B) \\ &\quad + 10\log_{10}(\text{NF}) + 10\log_{10}(\text{SNR}) \ \text{ [log]}, \end{aligned} \tag{1.3}$$

where k is the Boltzmann constant, T is the operating temperature in Kelvin, B is the equivalent noise bandwidth (ENBW) in Hertz, NF is the noise figure up to demodulator, and SNR is the required signal to noise ratio over the ENBW for the desired bit error rate (BER). The log version of the formula assumes room temperature. The goal of this section is to determine the required RX NF to meet the required sensitivity of -103 dBm at a BER of 10^{-3}. This requires computation of ENBW and SNR.

The optimal non-coherent demodulator for non-continuous phase M-ary FSK, where M=2 for conventional BFSK, and M=16 for 16-FSK, is shown in Fig. 1.2, assuming an additive white Gaussian noise (AWGN) channel. The optimal structure consists of M matched-filters followed by energy detectors, and a decision block that selects the path which has the highest energy in a given symbol period. The probability of error for M-ary FSK given this optimal structure is given by the following equation [Joh01]:

$$P_{error} = \frac{M}{2M-2} \sum_{j=1}^{M-1} \left(\frac{-1^{j+1}}{j+1} \binom{M-1}{j} e^{-\frac{j \log_2 M}{j+1} \frac{E_b}{N_0}} \right), \tag{1.4}$$

where E_b is the energy per bit in Joules, and N_0 is noise power spectral density in Watts/Hz. The BER resulting from this equation is plotted in Fig. 1.3 for both BFSK and 16-FSK. At a BER of 10^{-3}, 16-FSK enjoys a 4.87 dB advantage over BFSK. This is the principal motivation

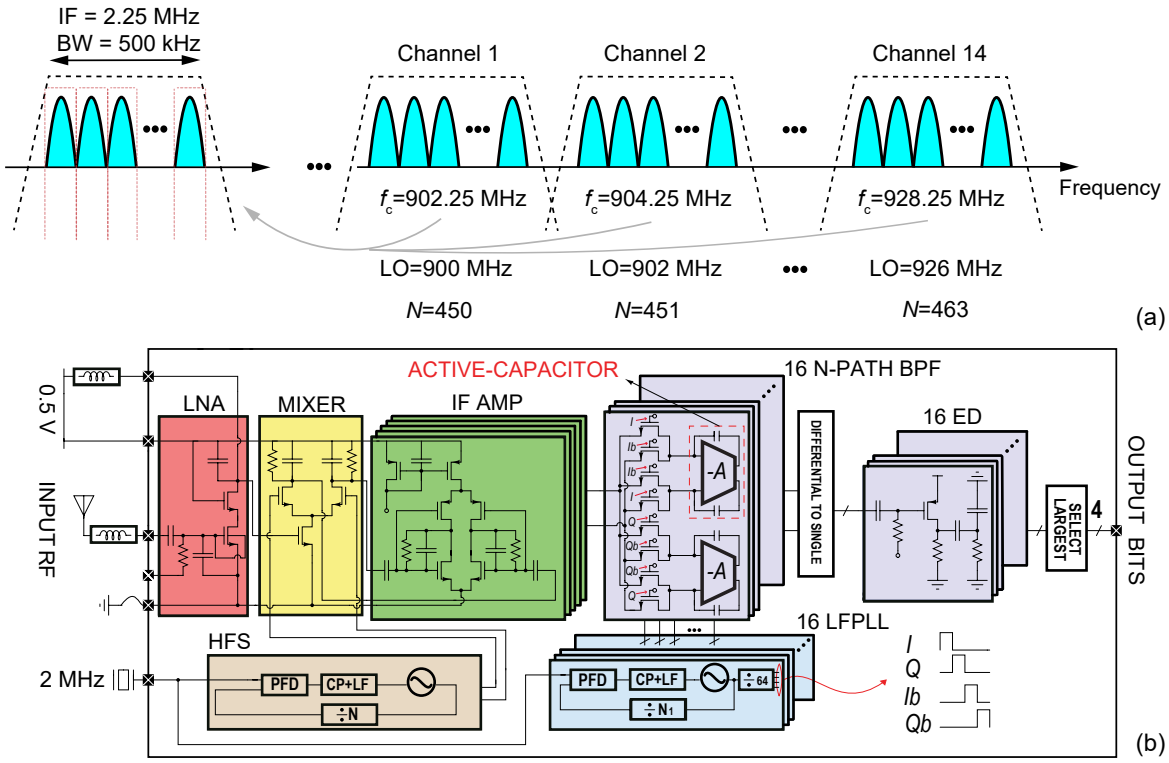

Figure 1.4. (a) Frequency plan for the proposed radio. (b) Receiver architecture.

for moving to a 16-FSK modulation format. Naturally, this has a trade-off: reduced spectral efficiency. For some applications, especially in remote areas with little-to-no existing wireless infrastructure, this may be an acceptable trade-off. Note that inclusion of coding, which also affects spectral efficiency, will be of interest in future work. Also, note that Gaussian filtering can be added to both BFSK and 16-FSK as an additional trade-off between performance and spectral efficiency, though spectral efficiency would be improved more with BFSK due to the lower symbol rate for 16-FSK (for the same data rate).

To compute the required NF, it is necessary to first compute SNR from E_b/N_0. This can be computed by multiplying E_b/N_0 by the spectral efficiency of the modulation scheme, noting that the bandwidth should be specified in terms of ENBW, not 3 dB bandwidth or null-to-null bandwidth:

$$SNR = \eta_{\text{spectrum}} \frac{E_b}{N_0}, \tag{1.5}$$

where η_{spectrum} is the spectral efficiency. The ENBW-based spectral efficiency for M-ary FSK is given by:

$$\eta_{\text{spectrum}} = \frac{\log_2 M}{M}. \tag{1.6}$$

For $M = 2$, $\eta_{\text{spectrum}} = 0.5$, and for $M = 16$, $\eta_{\text{spectrum}} = 0.25$. Thus, at 100 kbps, the ENBW of BFSK is 200 kHz, while for 16-FSK the ENBW is 400 kHz.

Per equations (1.4) and (1.5), an E_b/N_0 of 10.94 dB is required for a BER of 10^{-3} for BFSK, which translates to an SNR of 7.93 dB. Similarly, an E_b/N_0 of 6.07 dB for 16-FSK translates to an SNR of 0.05 dB. This is now sufficient information to compute the required noise figure:

$$\text{NF}_{\text{req}} = P_{\text{sensitivity}} - 10\log(kTB) - 10\log(\text{SNR}_{\text{req}}), \tag{1.7}$$

for $P_{\text{sensitivity}}$ in units of dBm.

For BFSK, $\text{NF}_{\text{req}} = 10.07$ dB, while for 16-FSK, $\text{NF}_{\text{req}} = 14.93$ dB. In other words, the required noise figure to implement a 16-FSK receiver is relaxed by 4.87 dB relative to that of a BFSK receiver for the desired specifications.

Importantly, as described in Section 1.3, there are no current reports of sub-mW BFSK receivers that achieve this type of NF at the desired data rate, and thus the 16-FSK approach offers a tangible advantage.

Note that since the bandwidth terms (B and the ENBW in the SNR_{req} term) end up cancelling out in the above analysis, the NF_{req} calculation can be simplified as follows:

$$\text{NF}_{\text{req}} = P_{\text{sensitivity}} + 174\text{dBm/Hz} - 10\log(R_b) - 10\log(\frac{E_b}{N_0}), \tag{1.8}$$

where R_b is the bit rate in units of bits/second.

1.5 Architecture of the Receiver

The proposed receiver is targeted for operation in the 900 MHz ISM band. To support multi-channel operation, the 26 MHz of bandwidth available in this band is split up into 14 channels, individually accessed by an integer-*N* PLL, which translates each channel down to an IF centered at 2.25 MHz as depicted in Fig. 1.4(a). Depending on the spacing between FSK tones, the 16-FSK signal occupies between 400-500 kHz of bandwidth. Sixteen individual filters are then required to filter each one of these potentially transmitted tones prior to energy detection.

1.5.1 RF Front-End

The overall receiver front-end is shown in Fig. 1.4(b). Incident RF signals to the antenna pass through an off-chip matching network that feeds an enhanced-g_m low-noise amplifier (LNA). The LNA utilizes a bondwire-based inductive source degeneration, and uses a dynamic threshold MOS (DTMOS) input through both the gate and the bulk to increase the effective transconductance by 20%. The LNA consumes 120 μW, which is 20% of the power consumption of the entire receiver. The LNA's noise figure is simulated to be 4 dB, and offers a gain of 21 dB.

The output of the LNA feeds a single-balanced mixer stage clocked by the high-frequency PLL. The PLL takes a 2 MHz crystal reference, and through integer division by $450-463$, mix-down the 14 channels to the 2.25 MHz IF. Since the receiver will perform non-coherent demodulation, low phase noise from the LO is not required, and therefore a ring VCO, which consumes less power and area than an *LC* VCO, is employed. The power consumption of the PLL is measured to be 245 μW, while that of the mixer is measured to be 12 μW.

After mixing down to the IF, five cascaded stages of IF amplifiers are implemented to further gain up the signal prior to demodulation. The IF amplifiers are designed to provide up to 60 dB gain at a power consumption of 7μW. Any number of IF amplifiers can be disabled to reduce gain for higher input signal power levels. The simulated noise figure from the antenna to the IF-amplifiers output is 14 dB.

1.5.2 Near-Optimal Ad-Hoc 16-FSK Demodulator

The ideal demodulator shown in Fig. 1.2 utilizes matched filters with impulse responses given by:

$$h_{matched}(t) = S(t-\tau)^*, \tag{1.9}$$

where $S(t)$ is the input signal to the filter, and τ is delay in seconds. It is not easy to build such filters, especially at low power consumption. As a result, a different, lower-complexity filter is thus required.

The lowest complexity filter that could work here is a two-pole bandpass filter, with transfer function given by:

$$H(s) = \frac{\frac{\omega_n}{Q}s}{s^2 + \frac{\omega_n}{Q}s + \omega_n^2}, \tag{1.10}$$

where ω_n is the natural frequency and represents the filter center frequency in radian$\times$Hz, and Q is the bandpass filter's quality factor. Sixteen such filters will have to be implemented as part of the demodulator.

Naturally, such filters will not have the same roll-off as an ideal matched filter, and will thus introduce non-ideal amounts of noise. In addition, such filters are not perfectly orthogonal, and will thus introduce distortion through inter-carrier and inter-symbol interference (ICI and ISI). For these reasons, performance is expected to degrade relative to a bank of ideal matched filters. Fortunately, a recent publication has shown that two-pole bandpass filters, when optimized, can yield performance (in terms of the required E_b/N_0 to achieve a BER of 10^{-3}) that is only 1 dB worse than ideal matched filters [XM20].

The optimization performed involves the following objective function:

$$\begin{cases} \text{minimize } P_e(E_b/N_0)_{\text{ideal}} - P_e(E_b/N_0)_{\text{proposed}} \\ \text{subject to } Q > 0 \;\&\; \omega_n > 0 \end{cases} \tag{1.11}$$

For a fixed tone spacing and a two-pole bandpass filter, there is only one variable to optimize: Q,

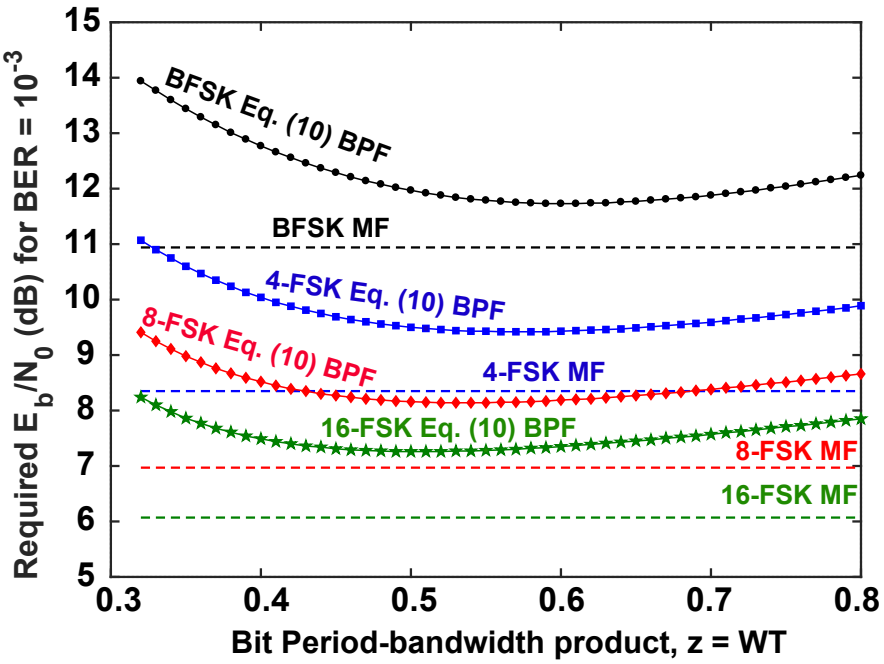

Figure 1.5. Optimizing the bandwidth of a two-pole bandpass filter for an ad-hoc M-FSK demodulator, (MF: Matched Filter) [XM20].

which ultimately sets the filter's bandwidth. A linear search across reasonable values of Q yields the required E_b/N_0 values for a 10^{-3} BER in Fig. 1.5 for various forms of M-ary FSK using a conservative upper-bound [XM20]. This figure shows that the required E_b/N_0 degrades at low values of filter bandwidths due to increased distortion, while also degrading at high values of filter bandwidth due to increased noise. The optimal normalized filter bandwidth for 16-FSK is 49% of the reciprocal of the bit period [XM20]. The resulting BER waterfall curve given this optimal filter design is shown in Fig. 1.6, illustrating the 1 dB degradation at a BER of 10^{-3} [XM20]. Similar analysis shows a 0.2 dB degradation when using two-pole filters for BFSK using actual BER curves, as shown in Fig. 1.6.

As a result of this degradation, the required noise figure calculated in Section 1.4 must be modified. Given two-pole filters, BFSK and 16-FSK now require an E_b/N_0 of 11.14 dB and 7.10 dB, respectively. This requires a now slightly more aggressive 9.86 dB noise figure for a BFSK receiver, and a 13.9 dB noise figure for a 16-FSK receiver. In other words, going

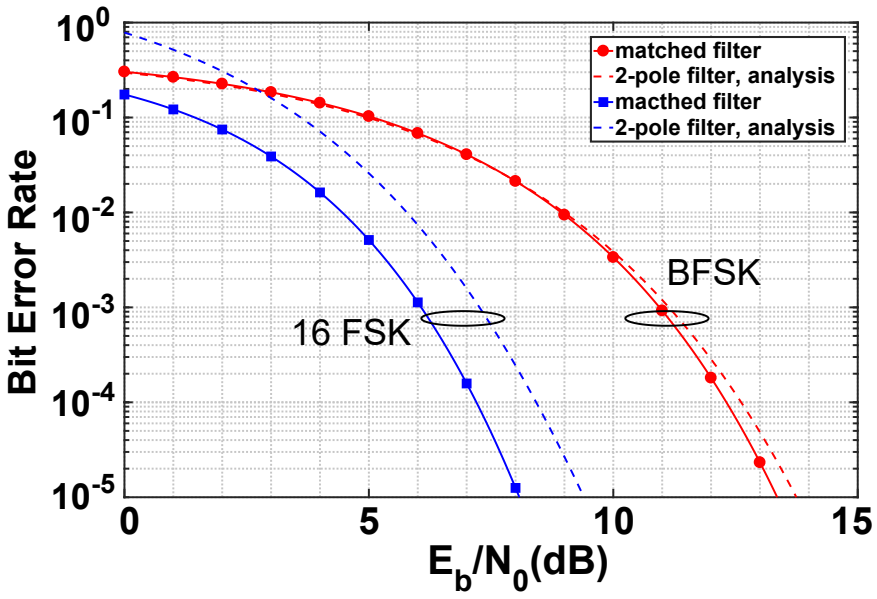

Figure 1.6. Bit error rate waterfall curves of analysed and simulated two-pole filters compared to an ideal matched filter for 16-FSK [XM20].

to two-pole filters reduced the 4.87 dB advantage of 16-FSK when using matched filters to a still-useful 4.04 dB advantage.

Note that this analysis assumes, for a 100 kbps data rate and 16-FSK, a 25 kHz spacing between tones/filter center frequencies, for 400 kHz of total bandwidth. Unfortunately, this analysis was completed after the chip design was finalized, and the proposed chip instead has a filter spacing of 31.25 kHz. This decreases the spectral efficiency slightly, though since the curves in Fig. 1.5 are shallow, the performance degradation is not substantial; as shown in Fig. 1.7, the difference is only 0.22 dB and 0.15 dB in BFSK and 16-FSK, respectively.

1.5.3 Bandpass Filter Implementation

Approach 1: $g_m - C$

There are many ways to implement bandpass filters with the transfer function of Eq. 1.10. However, Fig. 1.5 imposes one delicate and one loose constraint: 1) it is necessary to have extremely good control over the center frequency of each filter, especially in the presence of process-voltage-temperature (PVT) variation; and 2) it is necessary to have reasonably good

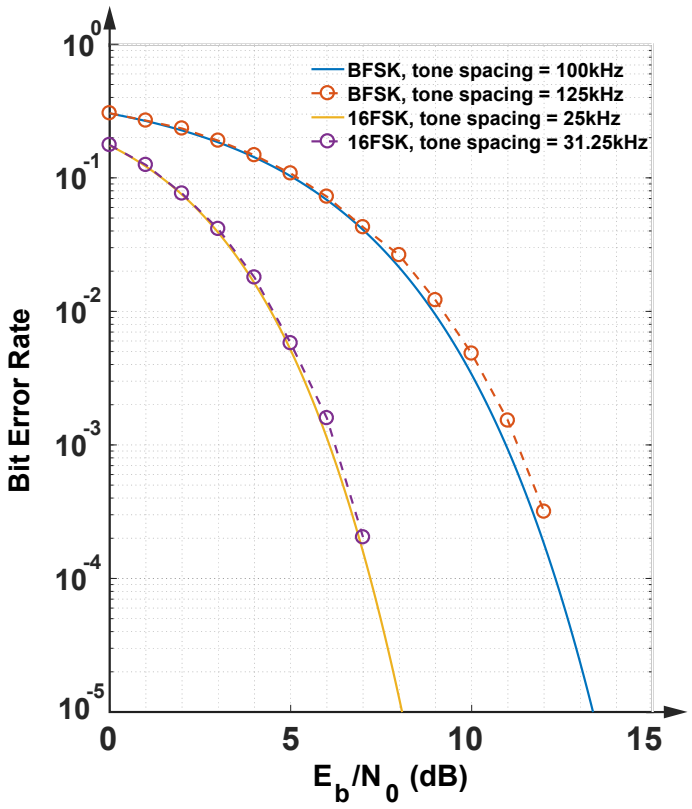

Figure 1.7. Probability of error versus E_b/N_0 for BFSK and 16-FSK and different tone spacing profiles.

control over the filter's Q-factor, though due to the shallowness of the curves in Fig. 1.5, the required precision here is not as important. Problem 1) is exasperated in 16-FSK, since unlike conventional designs which only require a few filters (e.g., two in BFSK), sixteen filters, all with precise center frequencies, are required for 16-FSK.

Due to PVT variation concerns, a conventional $g_m - C$ filter, such as the one shown in Fig. 1.8 (a), is not appropriate here. While the Q is well controlled by a ratio of capacitors, the center frequency is set by the transconductance and the absolute (square root) values of two capacitors. The capacitors will have large absolute process variation in their values (as opposed to typically small relative variation), while the transconductance will suffer from both absolute process variation, along with temperature and supply voltage variation. A simulation of the center frequency change, Δf, of a $g_m - C$ filter when temperature changes from 0 to 100°C,

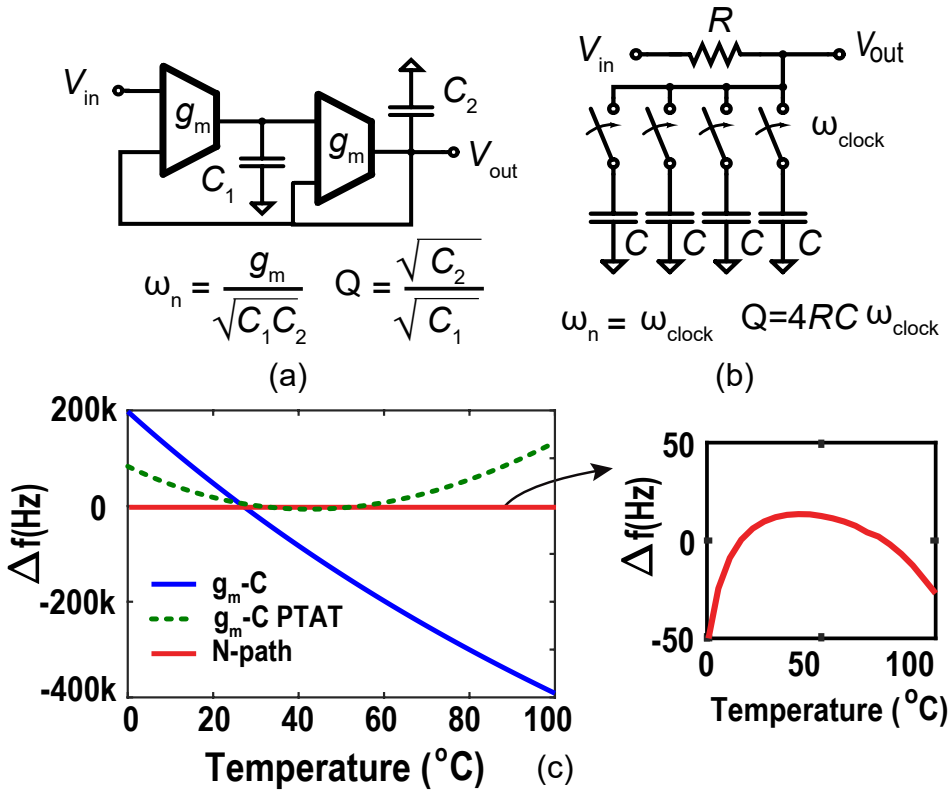

Figure 1.8. Band pass filter implementation using: (a) $g_m - C$ blocks, (b) a 4-path filter with center frequency at ω_{clock}. (c) The center frequency variation of each filter type versus temperature.

is shown in Fig. 1.8 (c). With a regular constant-current bias, the nearly 600 kHz variation is completely unacceptable, given the required 25-31.25 kHz filter spacing. Even when utilizing a proportional-to-absolute-temperature (PTAT) bias, the simulated $\sim$100 kHz variation is still unacceptable.

While it is certainly possible to tune $g_m - C$ filters, it is not straightforward to do so in an automated and low-power manner. For this reason, a different filter approach is needed.

Approach 2: N-path Filter

The main problem with the $g_m - C$ approach was that of analog circuit variation. To combat this, an N-path switched-capacitor filter can be instead used, as shown in Fig. 1.8 (b). By transitioning the switches sequentially at the desired center frequency of the filter, the capacitors

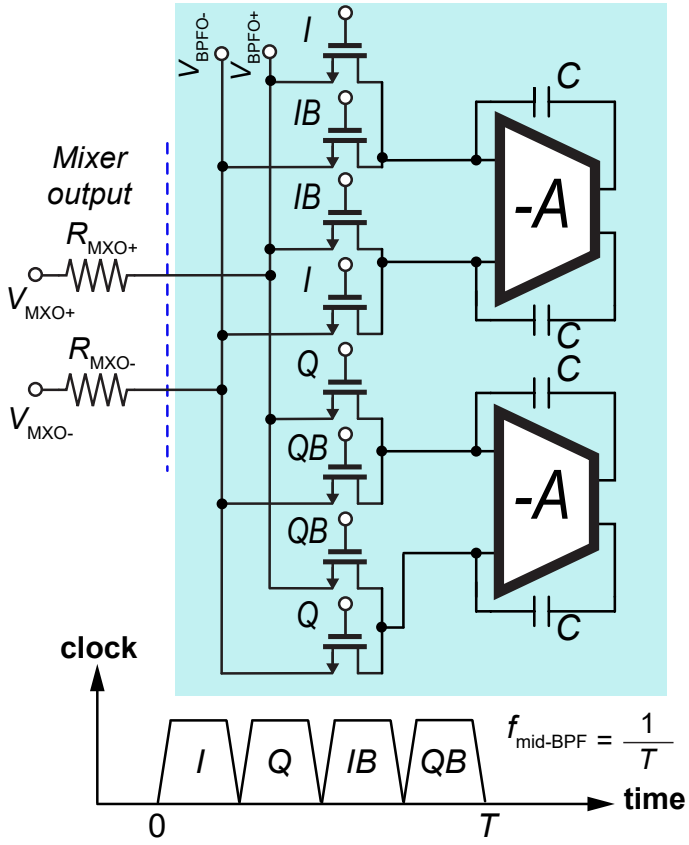

Figure 1.9. The 4-path filter design using the augmented Miller multiplication technique to save capacitor area.

will be amenable to keeping their charge relatively constant for input signals near the switching frequency, thereby presenting a high impedance at such frequencies, while requiring significant charging/discharging at frequencies away from the switching frequency, thereby presenting a low impedance at such frequencies [PR14]. As a result, the filter's center frequency is set by a switching frequency, which can be generated by a temperature-stabilized crystal oscillator passed through a PLL for frequency configurability. Thus, no center-frequency calibration is required, and the structure achieves a sub-50 Hz Δf per Fig. 1.8(c).

Going to an N-path filter arrangement does pose two challenges here in the pursuit of a low-power and low-area design: 1) the very narrow required bandwidths require large capacitors, and sixteen of these filters are required; and 2) sixteen different switching frequencies, each with multiple non-overlapping phase-separated replicas, are required to be generated.

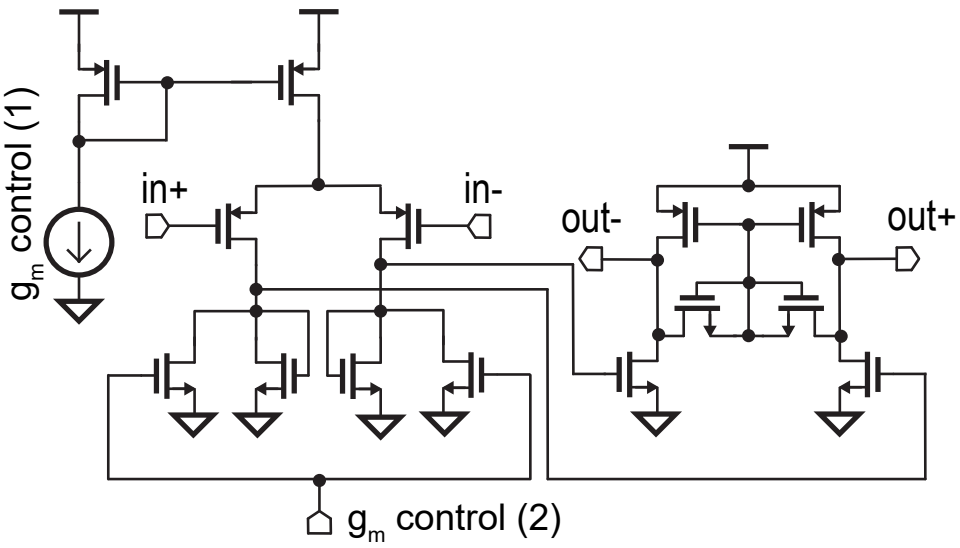

Figure 1.10. Circuit implementation of the low-power g_m stage for the augmented N-path filter.

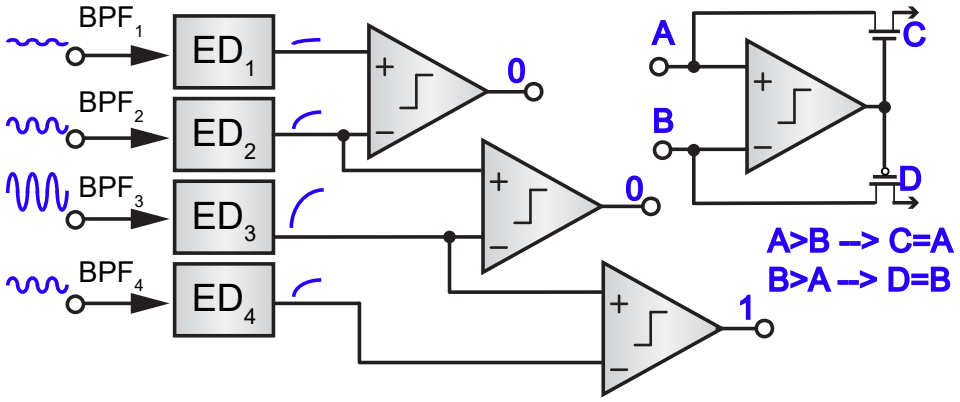

Figure 1.11. Select the largest algorithm for M-ary FSK where M=4.

The bandwidth of such an N-path filter is given by $(\pi NRC)^{-1}$, where N is the number of branches, R is the driving source impedance of the switches, and C is the baseband capacitor [Smi53]. Increasing N or R poses extra challenges on more complex multi-phase frequency generation circuits and pre-stage drivers, which increase power consumption or insertion loss. Instead, it is easier to increase C to achieve the required bandwidth.

In the proposed design, the switching frequency is fixed to the IF bandwidth of 2.25 MHz, and N is set to four, and the R is the output impedance of IF amplifier. Thus, to get the desired 31.25 kHz bandwidth, a capacitance of 20 pF is required. Since there are four capacitors in each

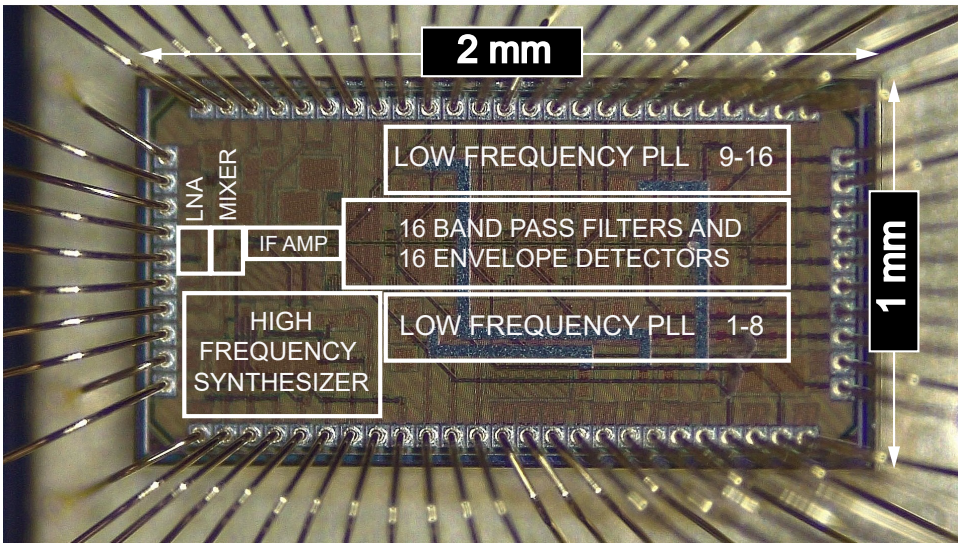

Figure 1.12. Die micrograph of the ultra-low-power 16-FSK receiver.

filter, and there are sixteen total filters, the total amount of required capacitance is 1280 pF. This is difficult to include on a single chip. Going off-chip is also impractical, since 64 individually accessible capacitors are required.

To address this and keep capacitance on-chip, Miller-boosting is utilized. Specifically, a small, yet lower-than desired capacitance is placed in a feedback loop with an amplifier with gain $-A_0$ [PR14]. This boosts the effective capacitance through Miller multiplication by $|A_0|$. The circuit implementation of an $N = 4$ filter is shown in Fig. 1.9, while the schematic of the employed amplifier, where both stages provide some voltage gain, is shown in Fig. 1.10. Since the capacitors only have to operate at baseband frequencies, the bandwidth of the required amplifiers can be low, resulting in a relatively low power overhead. In the proposed design, the amplifiers achieve a gain of 20 dB, which reduces the physically required total capacitance to 128 pF, saving 90% in on-chip area, all with only 32 μW total power overhead. Note that Miller multiplication can be turned off simply by shutting down the bias current of the amplifiers.

The second challenge posed by the use of sixteen 4-path filters is that each filter requires 4 non-overlap clocks, and each filter requires a different frequency. In the proposed design, this is accomplished through use of sixteen low-frequency PLLs tuned to 2 MHz through 2.5 MHz at

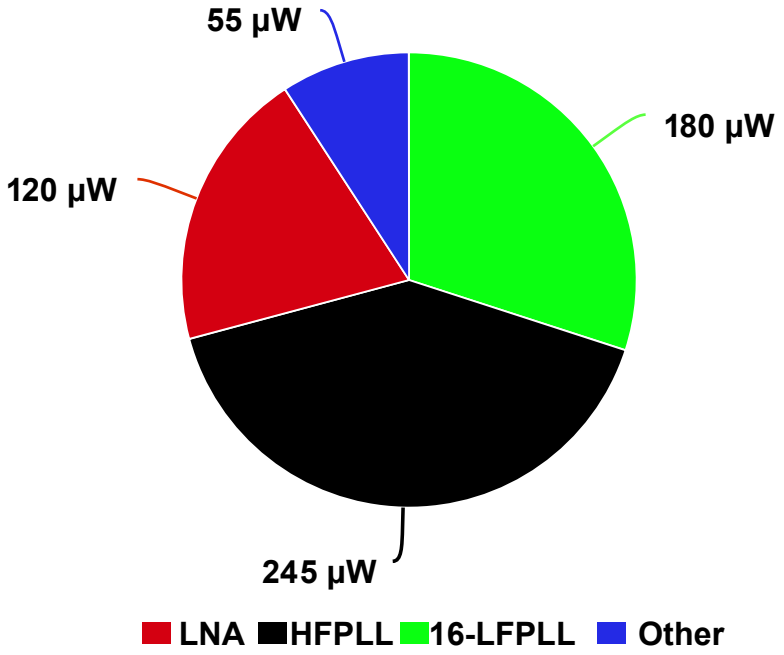

Figure 1.13. Power break down of the ultra low power receiver.

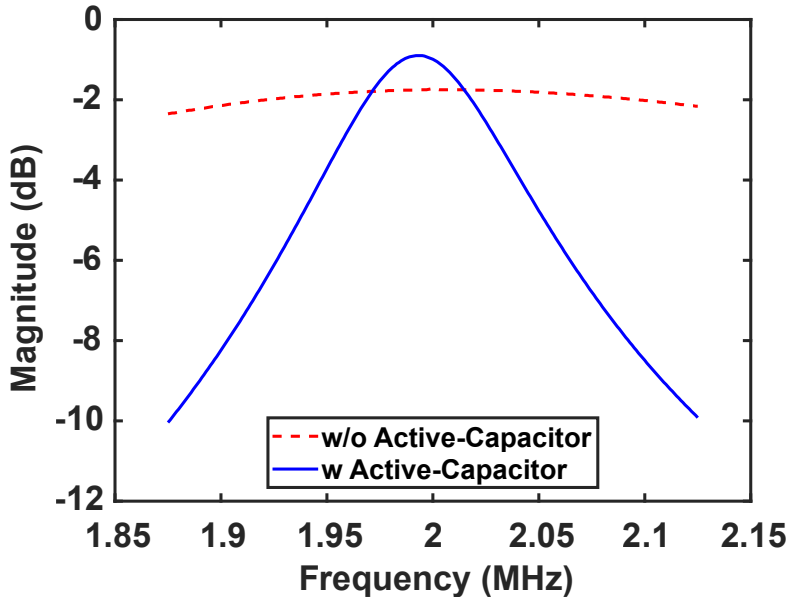

Figure 1.14. Simulated transfer function of the proposed N-path filter with and without the active capacitor approach.

31.25 kHz separation. Since the crystal reference is at 2 MHz, one possible solution would be to divide the crystal by 64 (to 31.25 kHz), and then build each PLL with divide ratios ranging

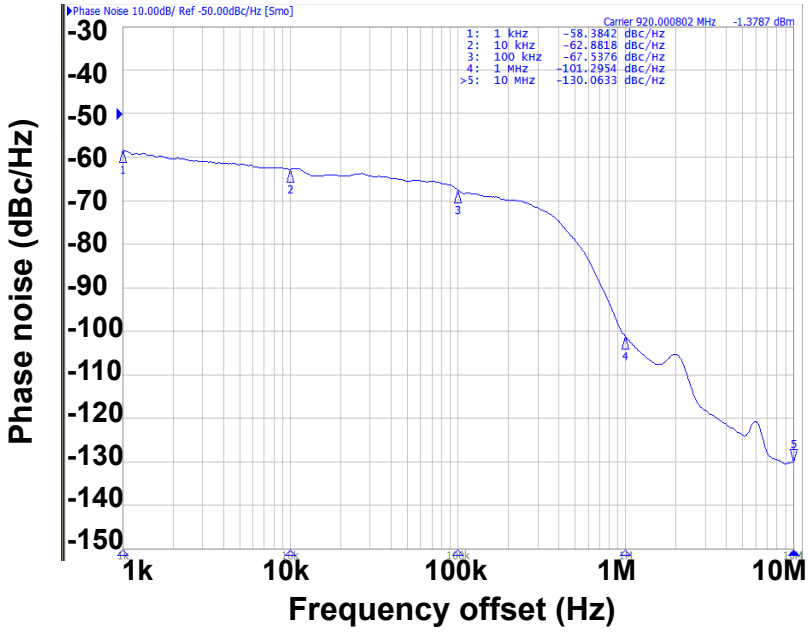

Figure 1.15. Measured high frequency synthesizer phase noise.

from 64 to 79. The low VCO frequencies here will result in very low power dissipation in each PLL. However, for loop stability reasons, each PLL's bandwidth should be less than or equal to $1/10^{\text{th}}$ the reference frequency - which in this hypothetical case would be 3.125 kHz [B. 12]. This requires the design of an enormous loop filter in each of the 16 PLLs, which is not feasible on a small, low-cost chip.

Instead, each of the low-frequency PLLs directly takes in the 2 MHz crystal as a reference input, and synthesizes frequencies at 2 MHz intervals between 128 MHz and 158 MHz using a conventional ring-VCO, integer-*N* divider, phase frequency-detector, charge-pump, and a loop filter (realizable on-chip due to the higher-frequency operation) structure, as illustrated in Fig. 1.4(b). To get the desired 2 MHz through 2.5 MHz signals, the VCO outputs are each then divided by 64 to produce the non-overlapped 4-phase I/Q signals. Each of the low-frequency PLLs were simulated to have a settling time of less than 50 μs. They were also laid out carefully to ensure critical wires are not routed close together, to ensure coupling and pulling is minimized, though the low-frequency nature makes this a relatively low risk.

The last stage divide by two (within the divide by 64 circuit) uses differential latches that

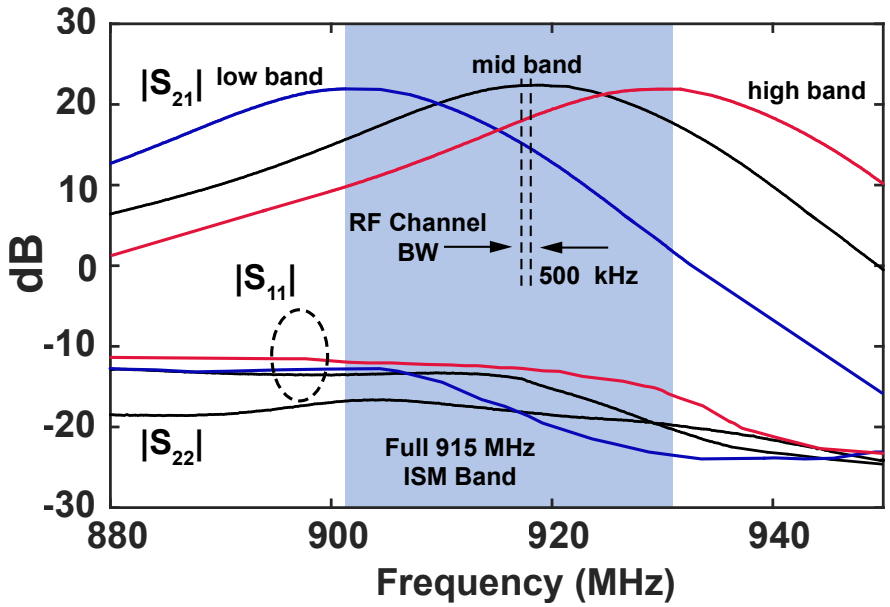

Figure 1.16. Measured low noise amplifier S-parameters for low, mid, and high channels.

I/Q signals can be generated from; the required 25% duty cycle waveforms are then generated by ANDing *I*-*Q*, *IB*–*Q*, $QB - I$, and *QB*-*IB*.

The cost of synthesizing the *N*-path filter clocks at initially higher frequencies is power: the sixteen low-frequency PLLs together consume 180 μW. However, this is a necessary cost to make the system realizable with minimal off-chip components.

1.5.4 Energy Detection and Demodulation Logic

The output of each filter is connected to an active envelope detector based on a subthreshold-biased common-source amplifier. Since the gain prior to the envelope detector is greater than 70 dB, the noise and conversion gain of the envelope detector is not restricted. As a result, all sixteen envelope detectors consume only 4 μW of power.

The select the largest circuit is the final stage in the receiver chain that detects the largest output between the 16 ED outputs. This has been done by comparing each output stage with the next one in orderly fashion. It starts by comparing the ED_1 and ED_2 outputs, and then compares the larger between those to ED_3 and up to ED_{16}. Fig. 1.11 reflects the implementation.

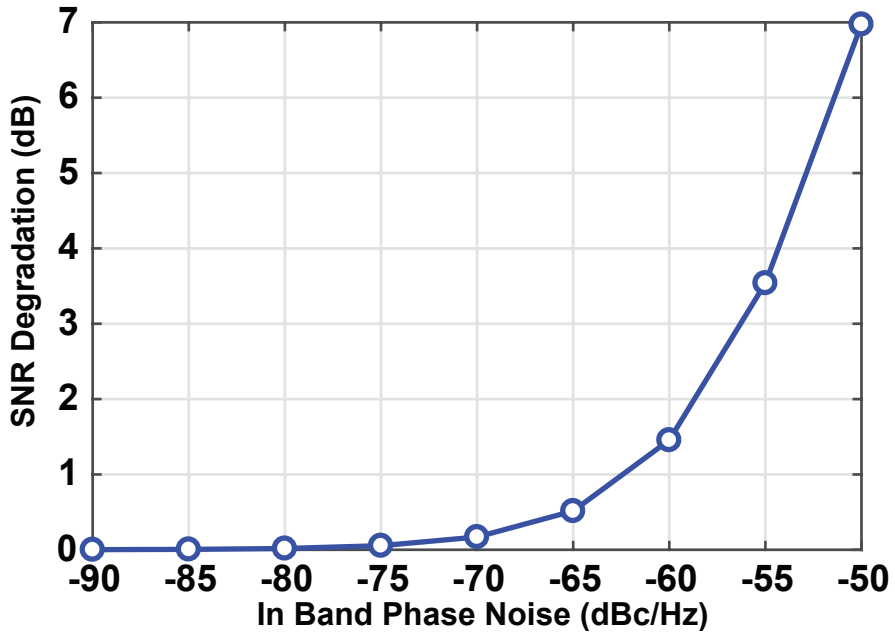

Figure 1.17. Mixer output SNR degradation due to in-band high frequency PLL phase noise.

1.6 Measurement Results

The receiver was fabricated in 65 nm, with a die area (including pads) of 2 mm^2 as shown in Fig. 1.12. At 0.5 V, the entire chip consumes 600 μW; a power breakdown is shown in Fig. 1.13. The LNA S-parameters are shown in Fig. 1.16 as measured through an on-chip unity-gain buffer, demonstrating an $|S_{11}| < -13$ dB and an $|S_{21}| > 20$ dB over the band of interest when tuning the LNA tank capacitance to support various channels. The LNA load inductor is implemented as an off-chip 10 nH inductor, while the source inductor is implemented with a bond wire with approximately 0.2 nH of inductance.

Fig. 1.14 shows the frequency response of a representative four-path filter with and without the active capacitor. As can be seen, Miller multiplication of the capacitor significantly sharpens the bandwidth from $\sim$300 kHz to 31.25 kHz. The phase noise of the high-frequency synthesizer generating the RF LO is shown in Fig. 1.15, indicating a phase noise of -100 dBc/Hz at a 1 MHz offset from carrier. According to simulated results in Fig. 1.17, SNR degradation due to in-band phase noise stays below 1 dB so long as in-band phase noise is less than -62 dBc/Hz.

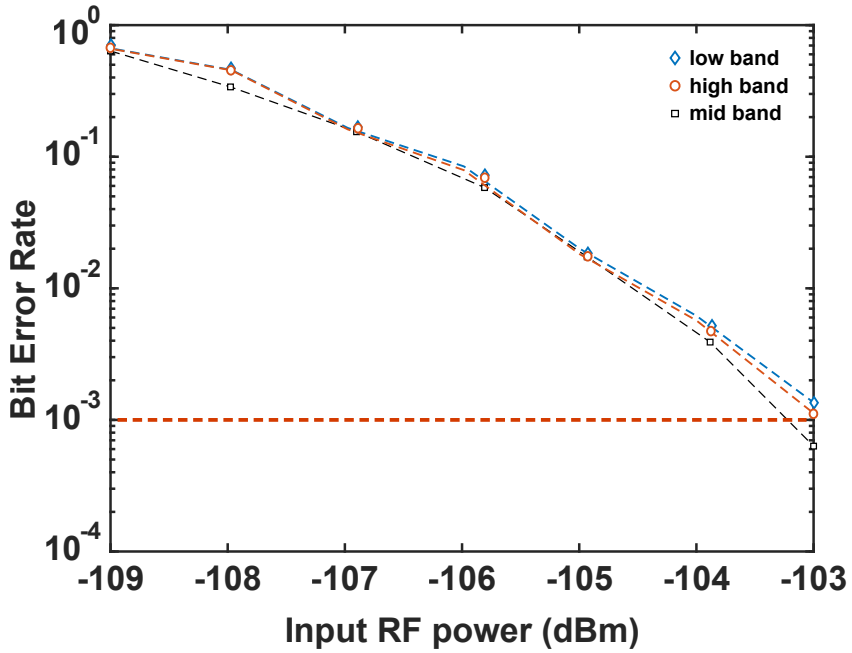

Figure 1.18. Measured bit error rate waterfall curves for operation at three representative channels.

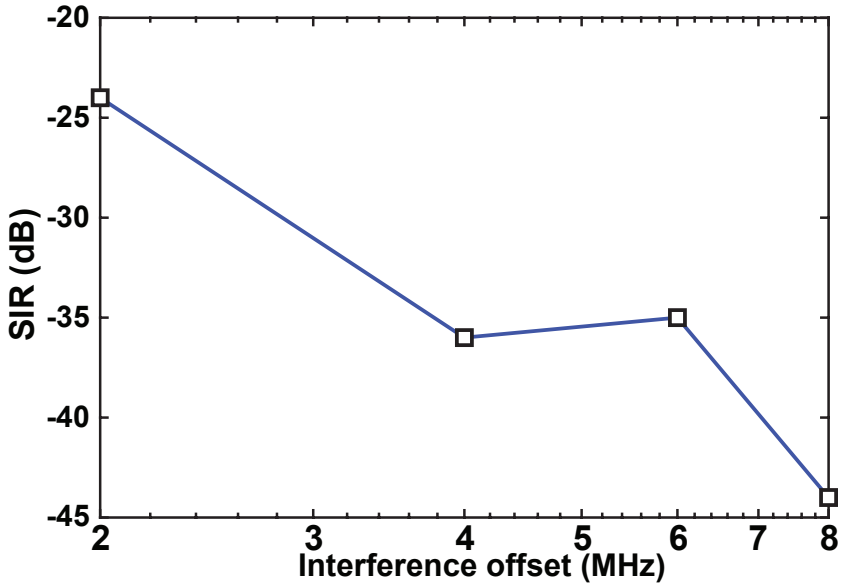

Figure 1.19. Measured signal to interference ratio.

The achieved better than -58 dBc/Hz in-band phase noise is thus acceptable in this non-coherent receiver, as also it goes down to -70 dBc/Hz at the 250 kHz edge of the channel.

The measured bit error rate waterfall curves for three operation bands (low-mid-high),

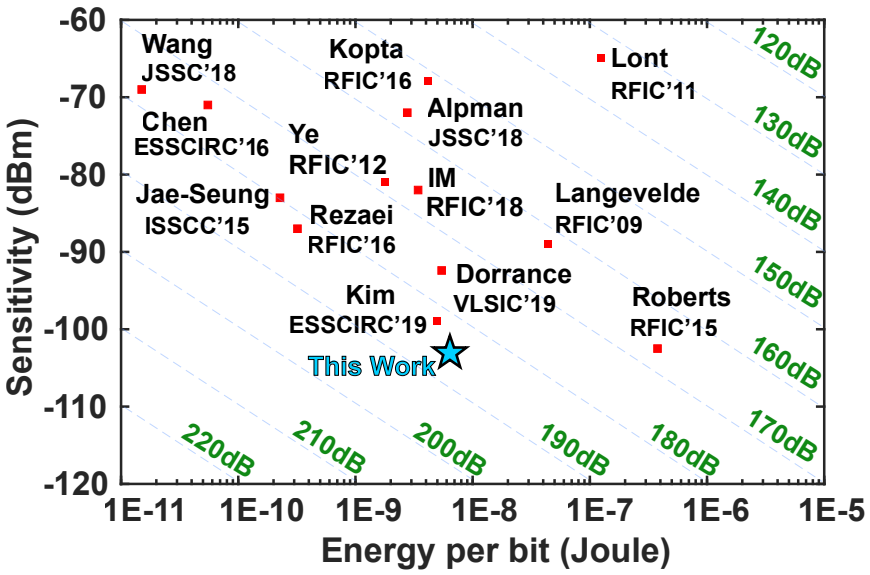

Figure 1.20. State of the art ultra low power receiver landscape. Lines of constant figures-of-merit are shown per Eqn. 1.1.

where band switching is realized in this case by tuning both the LNA tank capacitance and the high frequency synthesizer channel number, are shown in Fig. 1.18. For a data rate of 100 kbps, the receiver achieves a sensitivity of -103.2 dBm at a BER of 10^{-3} for the middle band. Given the 0.6 mW power consumption, the resulting figure-of-merit is 185.2 dB.

Fig. 1.19 depicts interference testing results, where the signal is placed 3 dB above the nominal sensitivity point, and the power of the CW interferer is raised until the BER drops back down to 0.1%. Compared to previously published work shown in Fig. 1.20, this work achieves the best figure-of-merit, and thus the best trade-off between power, sensitivity, and data rate. As aforementioned, this achievement does come at the cost of reduced spectral efficiency relative to other modulation schemes. The computed total receiver noise figure, based on the required E_b/N_0 for two-pole filters, is computed to be 13.76 dB, which is in line with the simulated receiver noise figure of 14 dB.

Table **??** summarizes the performance of the proposed receiver in more detail, and contrasts the results to relevant prior-art. Interestingly, the achieved sensitivity of -103.2 dBm at 100 kbps is 4.2 dB higher than the sensitivity in [KJC+19], also at 100 kbps, which is in line

with the improvement predicted by the analysis in Section 1.5.2. Due to the power overhead of the sixteen filters, the figure-of-merit improvement is limited to 3.2 dB. It should be noted that unlike many, though not all, other prior publications, the proposed design also includes the overhead and power consumption of a PLL uses to perform channel selection.

1.6.1 Notes on Receiver Dynamic Range and Filter Linearity

The receiver dynamic range is defined of the input power range received by the antenna in which the system can properly operate afterwards. The minimum detectable signal is set by the system noise figure and the maximum signal that can handle is set by usually the back-end blocks linearity such as IF amplifier. In the discussed application of point to point communication, the issue of handling large blocker signal is not eminent, unless a jammer signal is presented to obscure the communication. Measurement shown in Fig. 1.19 shows that with repsect to intererence the operating range with 3 dB desense is the -24 dBc at 2 MHz offset.

In system that have wide dynamic range, the input alternator is inserted within the chain, that can trade off the linearity with the noise figure for the cases in which the input signal to noise ratio is notably higher than the sensitivity level ($\geq$20dB). In the proposed receiver, for the operation with the input at the sensitivity level, back-end block such as the filter would have the input of the range below 10 mV, this would not cause the filter block go to compression. However, as you increase the input level, since there is wide range of gain control in the IF amplifier, therefore, we can control the signal received at the input of the filter not to push the filter in compression or generate inter-modulation products.

1.7 Conclusion

This chapter has shown that moving to a more power-efficient modulation scheme such as 16-FSK has both theoretical and practical benefits in terms of improving sensitivity at circuit-level power constraints. Specifically, theoretical analysis of two-pole filter-based demodulators for 16-FSK yields a 4 dB noise figure (or sensitivity) advantage compared to conventional

Table 1.1. Comparison with state of the art ultra low power receivers with data rates $\geq$ 10 kbps

	[vvv+09] RFIC'9	[YHW12] RFIC'12	[SLP14] RFIC'14	[KBE16] RFIC'16	[SJDL17] VLSIC'17	[IKW18] ESSCIRC'18	[KJC+19] ESSCIRC'19	[IKW19] TMTT'19	[LKD+19] RFIC'19	**This Work**
Process (nm)	130	90	90	55	65	40	65	40	28	**65**
Frequency (MHz)	915	2400	3000 - 5000	4000	2400	5800	915	5500-5800	2400	**920**
Supply (V)	1.2 - 1.5	0.8	1	1	0.6	0.5/0.95	0.9	0.95$^{\triangledown}$	0.6/0.9	**0.5**
Data Rate (kbps)	45	1000	200	100	25/50	62.5	100	62.5	62.5	**100**
Modulation	FSK	GFSK	WBFM	SCFDMA	FSK	OOK/FSK	BFSK	OOK	MC-OOK	**16-FSK**
SIR (dB)	NA	NA	-18	NA	-44/-45 @ +/- 3MHz	-24$^{\otimes}$	-14 @ 3MHz	-20$^{\otimes}$	-57/-49$^{\propto}$	**-24**$^{\otimes}$
Power (mW)	2	1.8	0.58	0.42	0.466	0.470	0.499	0.220	0.887	**0.6**
Sensitivity (dBm) @ 1E-3 BER	-89	-81	-80.5	-68	-102	-92.5	-99	-83	-92.6*	**-103.2**
Chip Area (mm^2)	1.5	0.42	0.89	0.4	1.48	1	2.25	0.45	0.19	**2**
Multi-Channel Capability	✓	X	✓	X	✓	X	✓	X	✓	✓
Integrated PLL	✓	X	X	X	✓	X	✓‡	X	X	✓
FoM† (dB)	162.5	168.4	165.0	151.8	179.3	173.7	182	167.5	171.1	**185.2**

†FoM (dB) $= -$Sensitivity (dBm) $+ 10\log_{10}$(Data Rate/1bps) $- 10\log_{10}$(Power/1W).
‡ Off-chip loop filter is used for PLL.
$^{\triangledown}$ 0.5V for VCO, 0.95V for analog blocks.
* 10% PER including packet acquisition and decoding performance.
$^{\otimes}$ Adjacent channel.
$^{\propto}$ CW blocker at 20MHz offset/20MHz Wi-Fi blocker at 25MHz offset adjacent channel.

BFSK modulation. To exploit this property, a 16-FSK receiver was designed in 65 nm, where a collection of sixteen N-path filters were used to perform the filtering necessary for demodulation of this signal. The chip was measured to consume 0.6 mW of power, and achieved a sensitivity of -103.2 dBm at a data rate of 100 kbps. This represents a 4 dB improvement over prior art at the same data rate, and when taking power overhead into account, a 3.2 dB figure-of-merit improvement. The proposed receiver achieves sufficient sensitivity to enable next-generation IoT and sensor network applications to operate in mesh network topologies, with nodes ideally consuming less then 1 mW while being spaced up to 1 km apart.

1.8 Acknowledgements

Chapter 1, in full, is a reprint of the material as it appears in Journal of Solid-State Circuits, 2021, Nikoofard, Ali; Abbasi-Zadeh, Hamed; Mercier, Patrick P., IEEE Press, 2021 and the material in Symposium of VLSI Circuits, 2020, Nikoofard, Ali; Abbasi-Zadeh, Hamed; Mercier, Patrick P., IEEE Press, 2020. The dissertation author was the primary investigator and author of these paper. I would like to acknowledge "Hamed Abbasi-Zadeh" of EEMS[1] lab as the

[1]Energy Efficient Micro-Systems

second author of the work and all his help during the measurement, and Patrick P. Mercier as the third author of the works.

Chapter 2

Low Power 16-FSK Transmitter

2.1 Abstract

This chapter shows a highly efficient transmitter capable of radiating GFSK and 16-FSK modulated signals in the 900MHz ISM[1] band. Multiple low power techniques are exploited such as a class-D VCO and a class-E single stage PA to enhance the Tx efficiency. Using an on-chip DC-DC converter, the VCO can operate with down to a 250mV supply and generate 750mV signals to the input of the PA. A phased locked loop (PLL) is implemented for rapid calibration of the LO frequency and is locked to a 2MHz crystal, which also provides the clock for the DC-DC converter. The fabricated integrated circuit occupies 1mm^2 area in 65nm LP CMOS, achieves a peak 76.2% PA efficiency and 63.9% Tx efficiency, while being capable of delivering up to 3dBm to a 50Ω antenna.

2.2 Introduction

Emerging IoT applications in smart agriculture, infrastructure monitoring, and distributed asset tracking require radios that operate over long ranges (e.g., ∼1km) yet consume low-power (e.g., ∼1mW). Since such applications may not operate near the presence of existing cellular-based infrastructure, they can be organized into ad-hoc mesh networks, where data is passed

[1]The ISM radio bands are portions of the radio spectrum reserved internationally for industrial, scientific and medical (ISM) purposes.

between nodes until arriving at a connected edge. As a result of such bi-directional network traffic, transceivers must be low-power in both the Rx and Tx modes. Since the noise figure of an Rx can only go so low, long range is typically achieved by increased Tx output power - which is not an acceptable solution when total Tx power consumption is constrained [MC15].

Under such constraints, recent work has explored the use of modulation schemes that theoretically require less SNR to demodulate than modulation schemes conventionally used in low-power radios such OOK and BFSK [WAI20c]. For example, [NZM21] utilized 16-FSK, which has a 4.87dB E_b/N_0 advantage over BFSK at BER$= 10^{-3}$, to enable achievement of -103dBm of sensitivity at 100kbps. Assuming a Tx output power of 0dBm, this achieved sensitivity is sufficient to close a 1km link at 900MHz. While such a modulation scheme has worse spectral efficiency than BFSK, this is an acceptable trade-off in many ad-hoc networks operating away from cellular infrastructure. However, there have not been any low-power 16-FSK Tx published in the literature and, more importantly, it is generally extremely difficult to achieve high Tx efficiency, defined as the ratio of output power and the total power consumed by the entire Tx, for any type of modulation at low output power.

The power consumption of transmitters that output relatively high power (e.g., $P_{out} \geq$ 10dBm or 10mW) are generally dominated by the efficiency of the power amplifier (PA). However, at the lower output powers generally of interest to low-power IoT mesh networks (e.g., $P_{out} \leq$ 3dBm or 2mW), the power consumption of peripheral blocks including LO generation, data modulation, PA buffers, etc., can be a large component of overall Tx power consumption, making achievement of high Tx efficiency challenging.

To reduce the overhead burden posed by local oscillator generation and modulation circuits, [YYY$^+$19] performed GFSK modulation with the entire circuit running at 0.2V, achieving a Tx efficiency of 25% at $P_{out} =$ 0dBm. However, this was targeted specifically to run on an energy harvester, and the overhead of generating such a supply voltage from a battery was not included. On the other hand, [CBY$^+$19] utilized a digital ring VCO, edge combiner, and switched-capacitor PA (SCPA) to achieve a state-of-the-art Tx efficiency of 32% at $P_{out} = -$3dBm. However, the

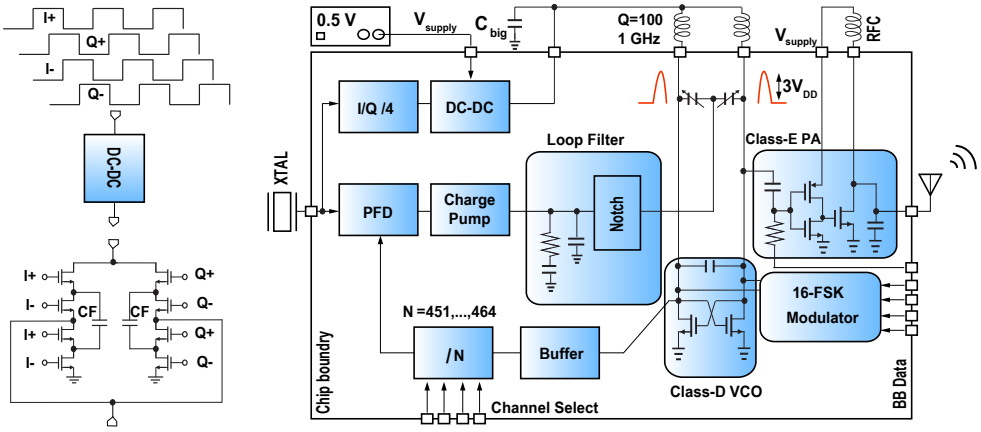

Figure 2.1. Block diagram of the proposed 16-FSK/GFSK transmitter.

employed SCPA's efficiency does not scale well across a wide output power range at a fixed VDD, which is desired in ad-hoc networks with variable inter-device spacing.

This chapter presents a transmitter that generates both 16-FSK and binary GFSK modulated signals with up to 63.9% Tx efficiency by: 1) efficiently performing LO generation via a 0.25V class-D VCO with high-Q off-chip inductors; 2) providing this 0.25V supply through an on-chip switched capacitor DC-DC converter operating with 71.6% efficiency; 3) exploiting the non-coherent communication link by running the VCO, which has <4kHz frequency drift over 10ms, open loop during packet transmissions; 4) including an on-chip PLL to perform rapid ($<50\mu$s) VCO calibration prior to the start of each packet; 5) directly modulating the VCO to provide a GFSK or 16-FSK signal without concern to PLL loop bandwidth and stability criteria; and 6) amplifying the resulting constant-envelope signal via a 76.2%-efficiency class-E PA.

2.3 Circuit Implementation

Fig. 2.1 shows the overall block diagram of the proposed transmitter. An on-chip 2MHz crystal oscillator is employed both as a reference to an on-chip PLL, and as the clock-source (after division to 500kHz) for a four-phase on-chip switched-capacitor DC-DC converter. The chip takes a single 0.5V supply as input, which is the main supply for all blocks except for

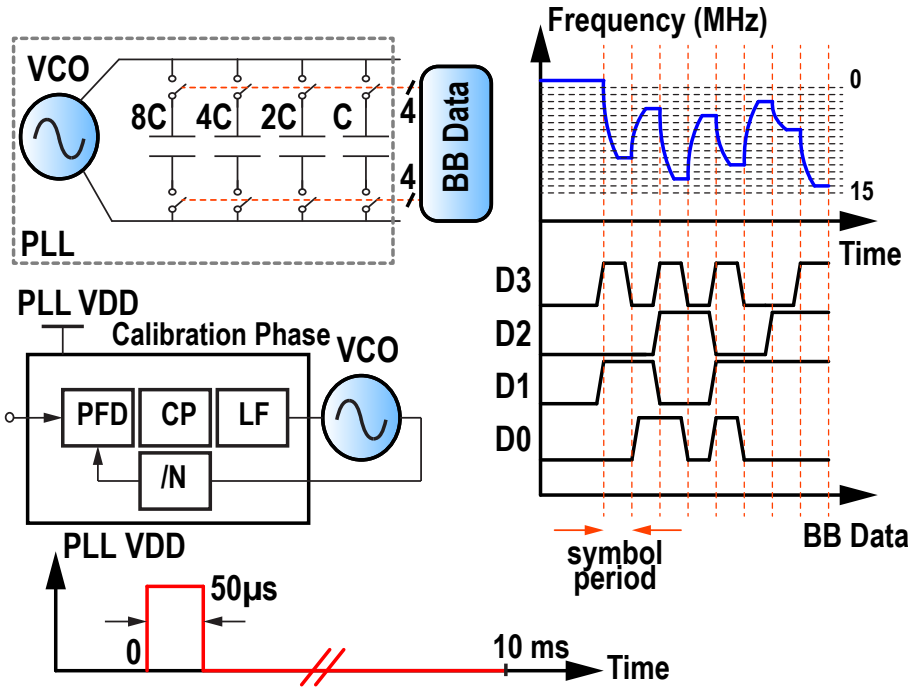

Figure 2.2. 16-FSK modulator with duty-cycled VCO calibration diagram and its representative baseband waveforms next to output frequency for 16-FSK

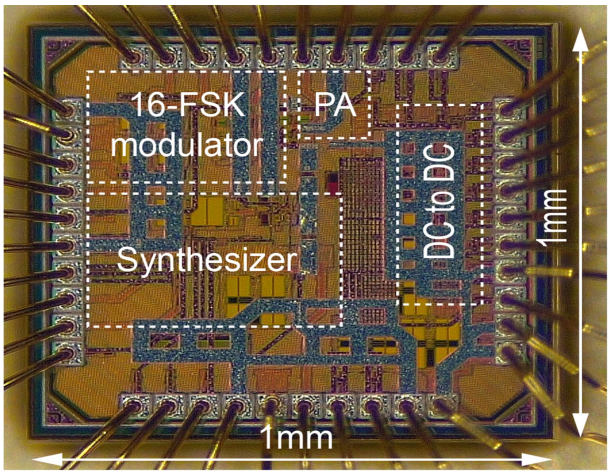

Figure 2.3. Die micro graph of the 16-FSK transmitter fabricated in 65 nm LPCMOS with a core area of 1 mm^2.

the VCO, which is instead powered directly from the DC-DC converter's output. The VCO is tuned by two capacitive DACs - one whose input comes from the PLL for channel selection, and the other whose input comes directly from the modulated data bits. The PLL has configurable

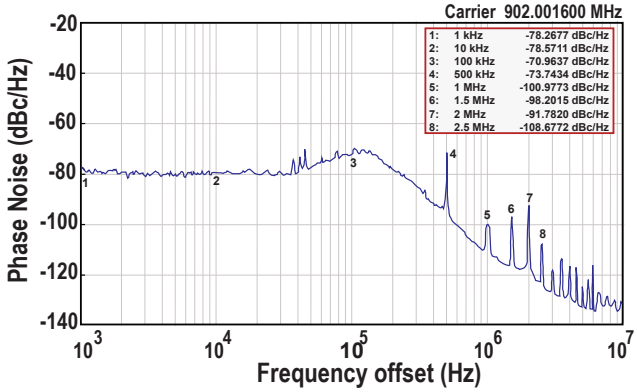

Figure 2.4. Measured VCO phase noise while locked via PLL and is power by Dc-DC converter all clocked with 2MHz reference.

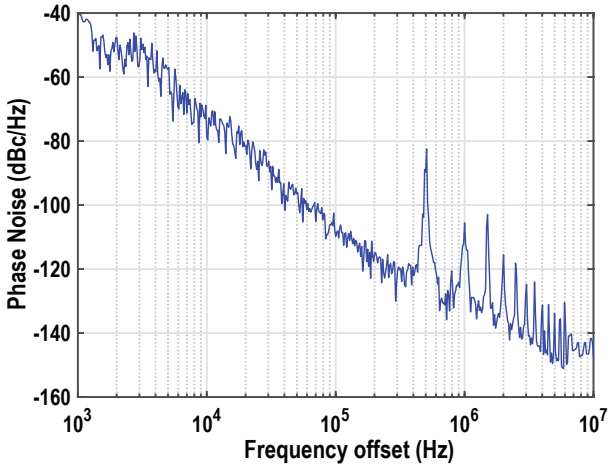

Figure 2.5. Measured open-loop VCO phase noise profile.

divider ratios to enable operation in one of 14 channels in the 902-to-928MHz ISM band. A RC-CR notch filter is placed inside the PLL's loop filter to help attenuate the 2MHz reference spur without affecting the loop stability.

Since the VCO consumes the lion's share of the Tx power besides the PA, reducing its power is critical. By removing the conventional tail current source, the VCO can be operated at a low supply voltage down to 0.25V when operating in class-D mode. This creates oscillations with an amplitude of $3V_{DD}$ [FA13], which in this case is 0.75V - still well within voltage rating limits of on-chip core transistors. While class-D VCOs are known to achieve excellent phase noise, due to the non-coherent nature of the expected FSK receiver excellent phase noise is not

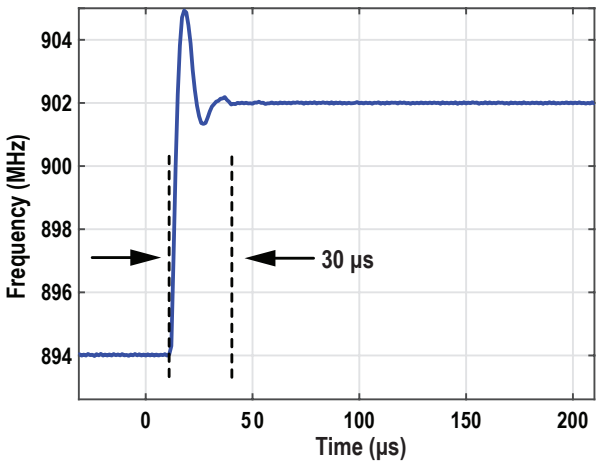

Figure 2.6. Measured transient response of the phased locked loop and its lock-time going from 894 MHz to 902 MHz.

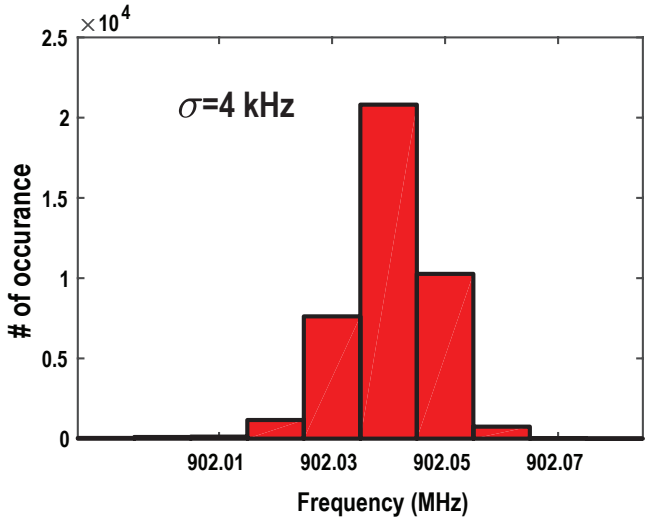

Figure 2.7. Open-loop VCO frequency stability measured over a 10ms packet.

required [AKW18], and thus the class-D operation was selected primarily for power reduction purposes.

As illustrated in Fig. 2.2, the PLL is activated at the beginning of each packet to calibrate the VCO's center frequency. Calibration is allotted 50μs to allow time for the PLL to settle. Once settled, the PLL circuits are power gated, and baseband data is directly passed to the VCO's 4b modulation C-DAC , which directly varies the tank's impedance in a time varying-manner,

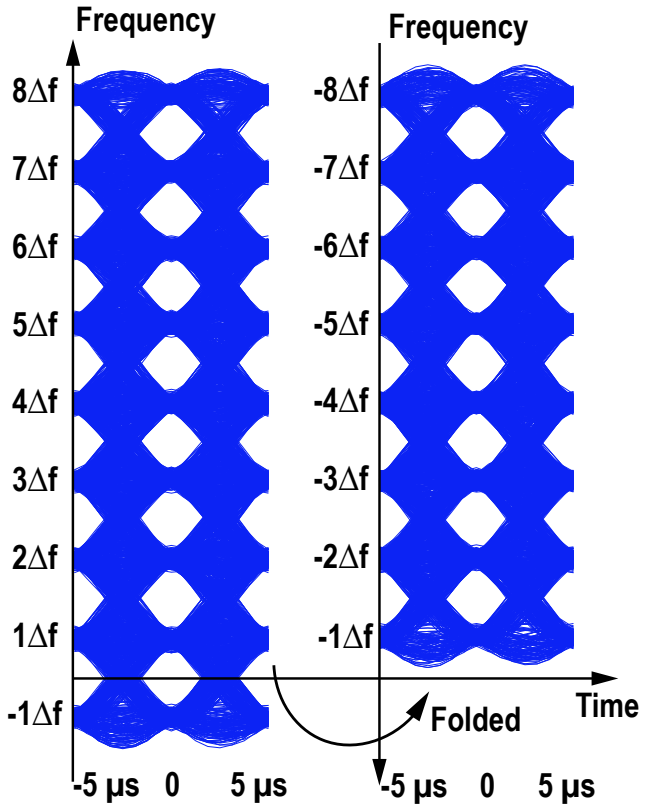

Figure 2.8. Measured eye diagram of 16-FSK modulation, Δf=31.25 kHz.

generating signals at one of 16 unique frequencies. The 4b C-DAC provides an LSB $\Delta f =$ of 31.25kHz, for a total frequency deviation of 500kHz within each channel. The baseband data can thus be delivered at a maximum rate of 31.25kS/s while maintaining orthogonality to ensure optimal demodulation, for a net data rate of 500kbps in 16-FSK mode. Alternatively, the 4b C-DAC can be used to deliver over-sampled GFSK data by consecutively switching between the 16 frequency levels in accordance with a Gaussian filter. In both cases the digital control signals are low-pass filtered before controlling the C-DAC switches to slightly slow down the transition time between frequencies via an exponential RC time constant to provide further filtering.

Using on-chip switching low frequency DC-DC converter, low voltage supply is provided to the class-D VCO. The DC-DC converter, uses two flying capacitors and a big off-chip load capacitor to offer a solid low-noise low-spur supply to the the VCO.

Thanks to the constant-envelope modulation scheme, the power amplifier is implemented

Table 2.1. Comparison with state of the art ultra low power transmitters

	Babaie JSSC' 16	Yin ISSCC' 18	Liu ISSCC' 18	Chen JSSC' 19	Weng RFIC' 20	This work
Technology node (nm)	28	28	65	40	65	65
Supply voltage (V)	0.5/1	0.2	1	0.6/0.9	0.5	0.5
Tx Frequency (MHz)	2050 to 2550	2420	2420	2400	430/915	920
Integration level	DCO+DPA +TDC	PLL+PA +μPM	ADPLL+AGC +PA	RO+ADPLL +DPA	DPA+TDC +IDAC	PLL+PA +DCDC
Modulation	GFSK	GFSK	GFSK	GFSK/FSK	16-QAM/BFSK	16-FSK
Tx Architecture	ADPLL Based	PLL Based	Single-point polar	RO Based all digital	ILRO	Open-loop w/PLL cal
PA Class	E/F2	E/F2	N/A	SC-DPA	DPA	E
PA Matching network	on-chip	on-chip	on-chip	partially off-chip	off-chip	partially off-chip
Tx Pout (dBm)	3	-0.25@ 0.2 V	-3	-9.4@0.6V/-3@0.9V	-10/-8.1	-3/0/3
Tx Pconsumption (mW)	4.4@ 0 dBm	4@ 0 dBm	3.2	1.55@ -3 dBm	0.533@ -15 dBm	1.3/1.9/3.1
PA Efficiency (%)	41	30	26.3	41@ 0.7 V	31.4/39	64.1/72/76.2
Tx Efficiency (%)	36@ 3 dBm	25@ 0 dBm	15.6@ -3 dBm	32@ -3 dBm	15.9@ -10 dBm	38.6/52.8/63.9
Phase noise @ 1 MHz offset (dBc/Hz)	-116 to -117	-119	N/A	-90	-104.5	-100.9
PLL Settling time(μs)	15	15	N/A	0.4 w 37.5 MHz xtal	N/A	30
PLL Largest spur (dBc)	-57	-47	N/A	-55	N/A	-73.7
Chip area (mm^2)	0.65	0.53	1.64	1	1.3	1

as a class-E PA with an off-chip RF choke. The matching network shunt and series capacitors are implemented on-chip while the series inductor is placed on a PCB.

2.4 Measurement Results

The proposed 16-FSK/GFSK Tx was fabricated in 65nm LP CMOS, occupying 1mm^2 of area including pads as shown in Fig. 2.3. Fig. 2.4 shows the measured phase noise of the VCO's output when the PLL is on, demonstrating a phase noise of -101dBc/Hz at a 1MHz offset, which is more than sufficient for non-coherent applications [AKW18]. As also shown in Fig. 2.4, the reference spur at 2MHz is only -91.7dBc thanks to the PLL's notch filter, while the DC-DC converter spur at 500kHz is only -73.7dBc.

During open loop operation, similar spurs levels are found as shown in Fig. 2.5, though out-of-band phase noise is improved. Fig. 2.6 shows that the PLL settles within 30μs, while Fig. 2.7 indicates that the VCO's stability while running open loop is <4kHz over a 10ms packet interval, which is more than sufficient given the 31.25kHz/500kHz tone spacing in 16-FSK/GFSK modes. Fig. 2.8 shows the measured eye diagram of the Tx output for 16-FSK, while GFSK is shown in Fig. 2.9. Both demonstrate wide open eyes, with FSK frequency errors of 4.2% and

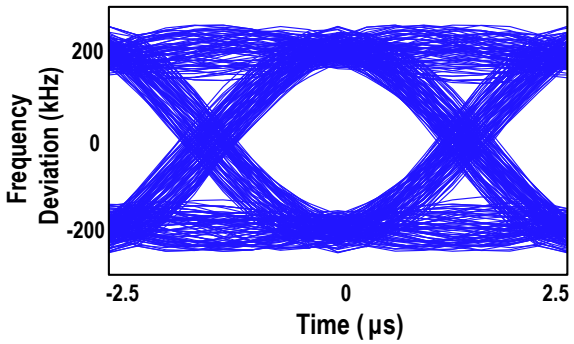

Figure 2.9. Measured eye diagram of GFSK modulation, Δf=200 kHz.

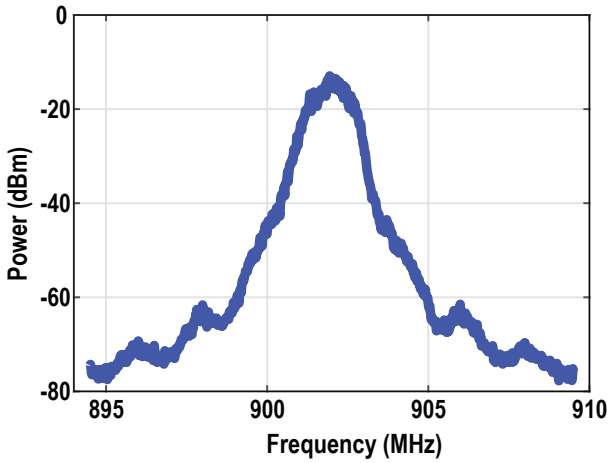

Figure 2.10. Measured 16-FSK spectrum.

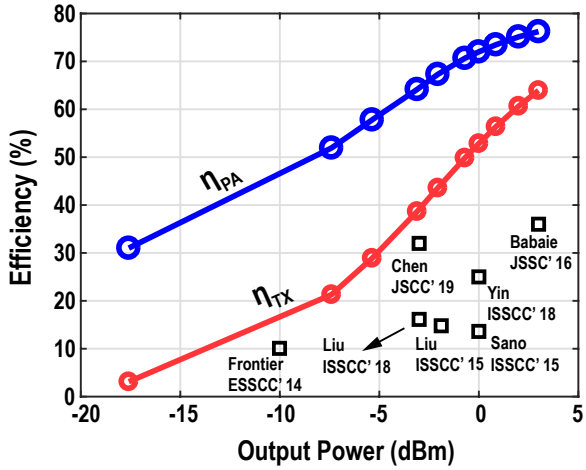

Figure 2.11. Efficiency of the proposed PA (blue) and the overall Tx efficiency (red) compared to the Tx efficiencies reported in the literature.

4.4%, respectively. Fig. 2.10 also shows the spectrum for 16-FSK, indicating a sharp, >50dB roll-off at a 2.5MHz offset.

Thanks to the careful class-E design and high-Q components, the PA is measured to achieve a maximum power-added efficiency of 76.2% when outputting 3dBm as shown in Fig. 2.11. The efficiency is still 72% and 64.1% at 0dBm and -3dBm, indicating the ability to still work efficiently even at back-off. At 0.25V, the VCO consumes 357.6μW, and thanks to the 71.5%-efficient on-chip switched-capacitor DC-DC converter, the power consumption is only 500μW including the converter. The PLL consumes 350μW during active mode (not including the VCO), but since it is on only for 50μs out of a 10ms packet, it's average power is only 1.75μW during a packet. The total average power during transmission is 1.3mW, 1.9mW, and 3.1mW at -3, 0 and +3dBm output power, representing state-of-the-art Tx efficiencies of 38.6%, 52.8%, and 63.9%, respectively, as illustrated in Fig. 2.11. Table. 2.1 compares the Tx performance with state-of-the-art low power transmitters.

2.5 Conclusion

The proposed Tx is capable of generating 16-FSK signals for use in long-range ad-hoc networks with relaxed SNR requirements. Moreover, utilizing low power and low voltage techniques, the transmitter designed in 65nm LP CMOS is capable of delivering up to 3dBm power with 63.9% system efficiency, which makes the radio suitable for long-range IoT mesh networks where low-power in bi-directional modes is required. This has been achieved via an on-chip DC-DC converter which is the supply for the class-D VCO followed by single-stage class-E power amplifier with a low-loss off-chip matching network.

2.6 Acknowledgments

Chapter 2, in part is currently being prepared for submission for publication of the material. Nikoofard, Ali; Mercier, Patrick P. The dissertation author was the primary investigator

and author of this material.

Chapter 3

Enhanced Privacy WiFi/BLE Transmitter

3.1 Abstract

Mobile phones, wearable, and other personal devices that use Bluetooth Low Energy (BLE) for communication offer exciting opportunities to connect with the world around us. Unlike cellular, WiFi, and most other conventional wireless communication technologies, BLE devices find and pair with each other by broadcasting beacon signals in the form of advertising packets. While this enables an easy and convenient way to network, this underlying concept poses significant privacy challenges. In this chapter, methods of enhancing the user privacy in transmitters that use m-QAM or GFSK modulation is presented. The approach is to obfuscate the Tx output signal features that can be classified easily by adversaries. Those features are carrier(center) frequency and I/Q offset. It has been shown that the proposed idea delays the user classification by adversaries from few seconds to more than 5 hours for more than 75% accuracy of classification.

3.2 Introduction

Many common consumer electronic devices broadcast 10s to 100s of BLE packets every minute. Thus, it is possible for a nefarious agent to stalk a user by placing BLE receivers in locations the target is likely to visit, and identify the target's presence, movement, and activities simply by observing their beacons. To combat this at the digital layer, crypto-graphic techniques

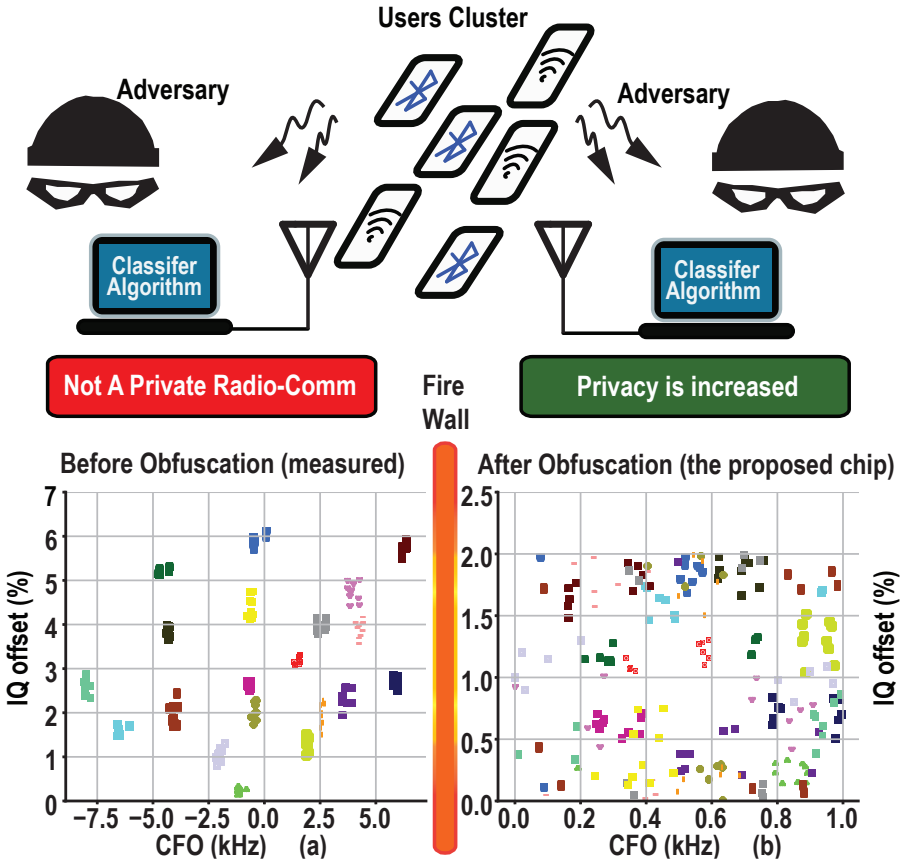

Figure 3.1. Privacy exposure of BLE transmitters, before and after obfuscation.

can be used, for example by periodically re-encrypting their MAC addresses. However, this does not offer a holistic solution: there are still identifiable signatures unintentionally embedded in the physical layer communication circuits that an adversary can use machine learning classifiers to study and eventually decipher. Specifically, recent work identified that the carrier frequency offset (CFO) and I/Q offset, and to a lesser extent I/Q imbalance of commercial BLE transmitters, which are almost exclusively built using I/Q architectures for integration into a WiFi/BLE combo chip for cost saving purposes, have subtle process variations between manufactured units that enable physical-layer fingerprinting by an adversary. Fig. 3.1 shows measured data from a collection of 20 different BLE units from the same manufacturer, showing clear, distinguishable features between all 20 units. It was estimated that an adversary can learn and identify such devices with 97% accuracy after 1 seconds. Despite such a clear privacy flaw, no prior-art ICs

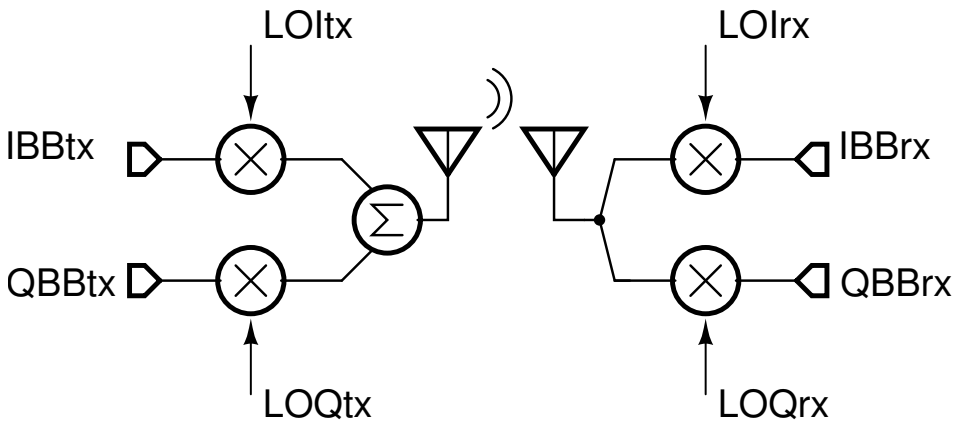

Figure 3.2. Generic I/Q transmitter with its own imperfections.

have demonstrated the ability to obfuscate these important physical-layer parameters to enable true privacy for users of BLE devices.

This chapter's design demonstrates a BLE-compatible Tx that utilizes the same type of I/Q modulator structure as employed in common BLE/WiFi combo chips, but with features to adjust and randomize both CFO and I/Q offset. The goal is to turn the clearly identifiable map in Fig. 3.1(a) to a muddied and difficult to identify map as illustrated in Fig. 3.1(b).

3.2.1 I/Q Offset Analysis

Imperfections in quadrature-modulation results in I/Q offset in which the adversary can classify with its own algorithm and ID the user. To obfuscate the transmitter I/Q offset, first an analysis is shown in which demonstrates the dependency of I/Q offset to the transmitter parameters and their strength or sensitivity. Let's consider a generic I/Q transmitter and receiver as shown in Fig. 3.2. Now, the set of equations can be written as

$$IBBtx = A \times cos(\omega_{BB}t + \phi_{cons,BBtx} + \phi_{err,BBtx}), \tag{3.1a}$$

$$QBBtx = A \times sin(\omega_{BB}t + \phi_{cons,BBtx}), \tag{3.1b}$$

$$LOItx = B \times cos(\omega_{LO}t + \phi_{cons,LOtx} + PN + \phi_{err,LOtx}), \tag{3.1c}$$

$$LOQtx = B \times sin(\omega_{LO}t + \phi_{cons,LOtx} + PN), \tag{3.1d}$$

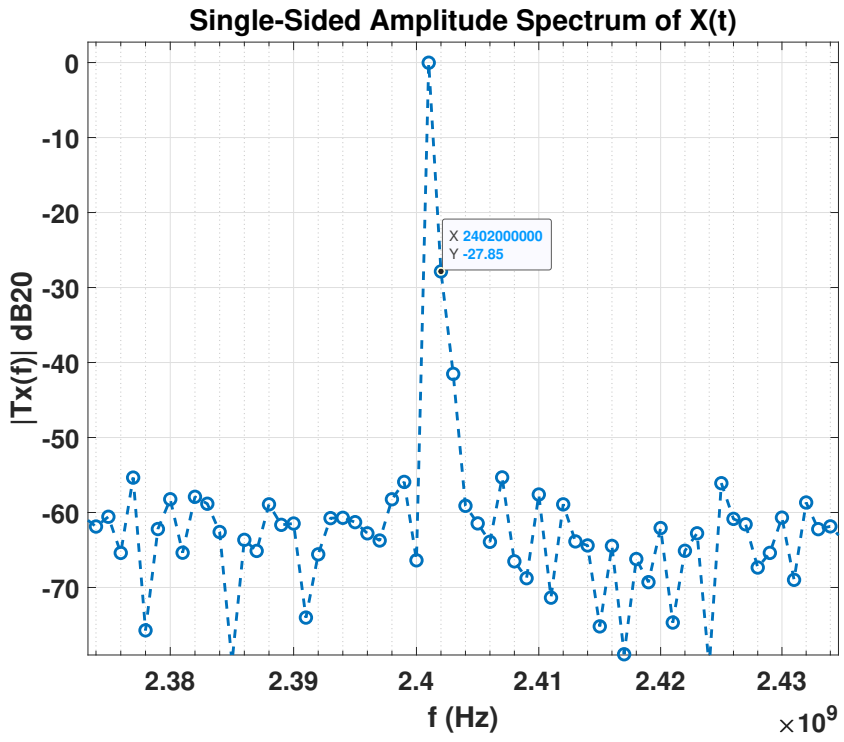

Figure 3.3. single side-band amplitude spectrum of Tx signal.

where in set of Eq. 3.1, ω_{BB} and ω_{LO} are base-band(BB) and LO frequencies respectively, the gain errors of I/Q BB and LO assumed negligible, however the relative phase difference and phase error of I/Q and LO is shown as $\phi_{cons,BBtx}$, $\phi_{cons,LOtx}$, $\phi_{err,BBtx}$, $\phi_{err,LOtx}$ respectively, and finally *PN* represents the LO phase noise. Therefore, the transmitted signal can be written as

$$Tx_{sig} = X(t) = IBBtx \times LOItx \pm QBBtx \times LOQtx + \alpha \times LOQtx, \tag{3.2}$$

where in Eq. 3.2 $\pm$, results in lower or upper side-band modulation and the last term represent the LO feed-through. As an example, the single side-band amplitude spectrum of the Tx signal for $\omega_{BB} = 2$ MHz, $\omega_{LO} = 2400$ MHz, $A = B = 1$, all constant phases equal to zero, $\phi_{err,BBtx} = -\pi/90$, $\phi_{err,LOtx} = \pi/180$ and $\alpha = 4\%$, will results in Fig. 3.3 single-sided amplitude spectrum of the Tx signal. As it can be seen from Fig. 3.3, the single side-band modulation is occurred at lower side-band (LSB), the LO feed-through is -27.85 dBc and the upper side-band (USB) due to phase

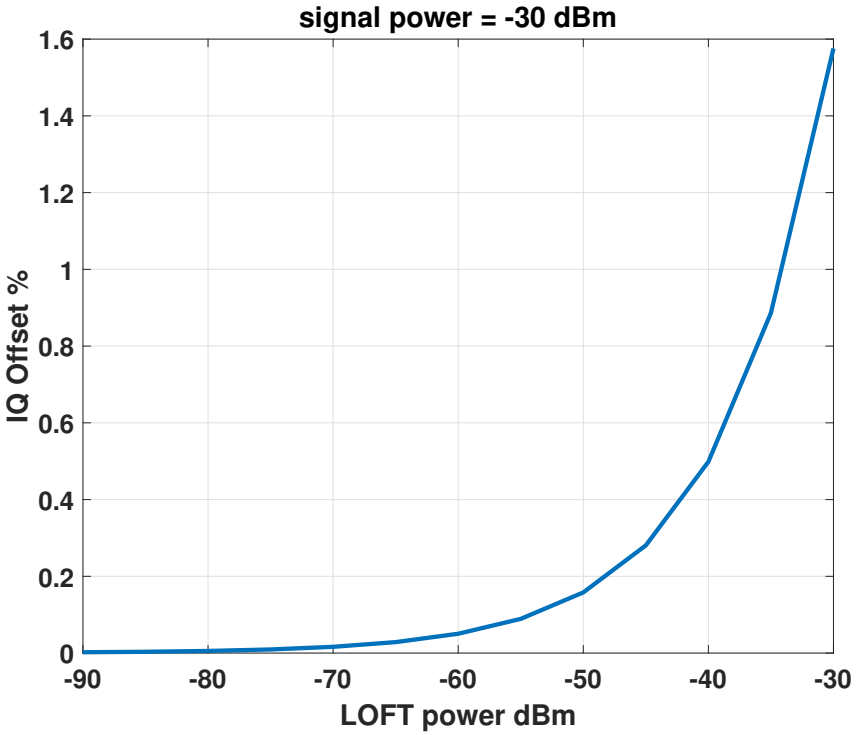

Figure 3.4. I/Q offset magnitude versus LOFT power in dBm.

error is at -41.52 dBc, and the noise floor is shown for 1 MHz resolution band width (RBW) and 4 degrees rms phase noise.

The I/Q offset stems from the I/Q constellation shifting away from the center of the I/Q plane at (0,0) indices. To understand how to obfuscate I/Q offset, first a knob is required to randomly change the I/Q offset. The LO feed-through is a known-factor that can cause the I/Q offset. To show the effect of LO feed-through on I/Q offset, consider set of equations shown in Eq. 3.1 in which the A is set at nominal value and B is increased from small numbers up to A. Fig. 3.4 demonstrates the fact that I/Q offset magnitude is very small at low LO feed-through (-60 dBc) and it increases as the LO feed-though increases. In the adversary perspective, the I/Q offset can only represent the magnitude since its phase depends on relative down conversion of the LOrx. Fig. 3.5 shows that when the LO feed-through increases, the center of the circle also deviate from the I/Q origin. In Fig. 3.5, the radius of the circle is the function of single side-band signal power and the circle's center depends on the relative power of the LO feed-through and

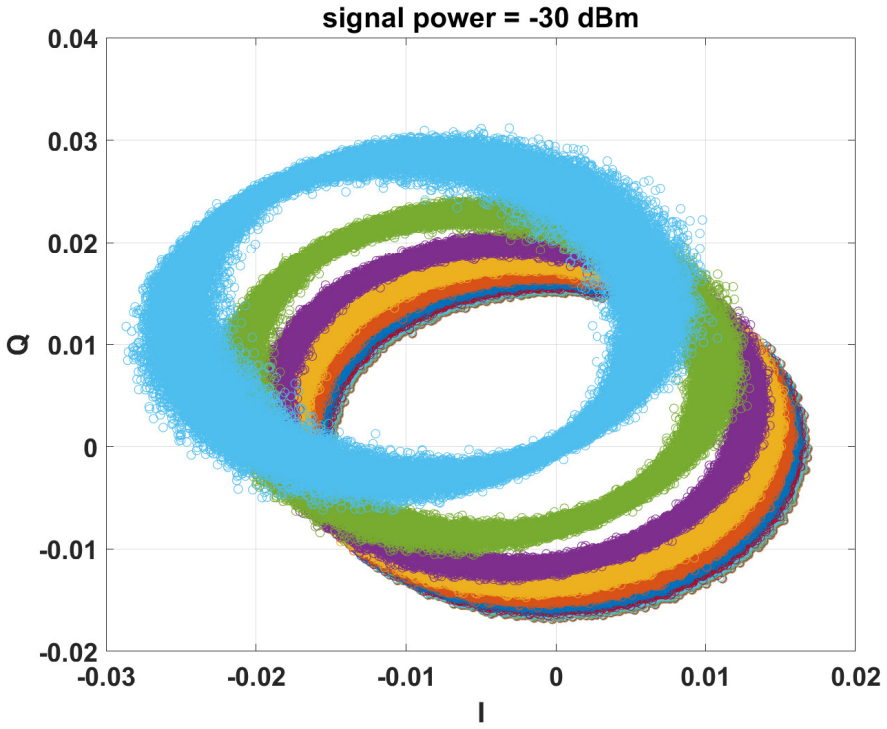

Figure 3.5. GFSK I/Q constellation versus LO feed through, from the center to the blue, LO feed-through has been increased to -30 dBm.

signal itself. Since the analysis proves the effect of the LO feed-through on I/Q offset, in Sec. 3.3 a technique is proposed to implement the aforementioned approach by randomizing the LO feed-through.

3.2.2 CFO Analysis

It has been observed that CFO plays the most important role for signal obfuscation. Since changing the VCO frequency when the PLL is closed would cause the VCO instantaneous frequency to go back to the desired channel within roughly 100$\times$ the reference cycles, in this case 25μs which is less than 10% of the packet duration, this would not be an applicable option. Therefore, the PLL needs to be opened, and then VCO frequency can be changed by adding or removing infinitesimal capacitor from the LC tank, transmit the packet and then PLL will be closed again.

The challenge however rises when the change of the VCO frequency should be from

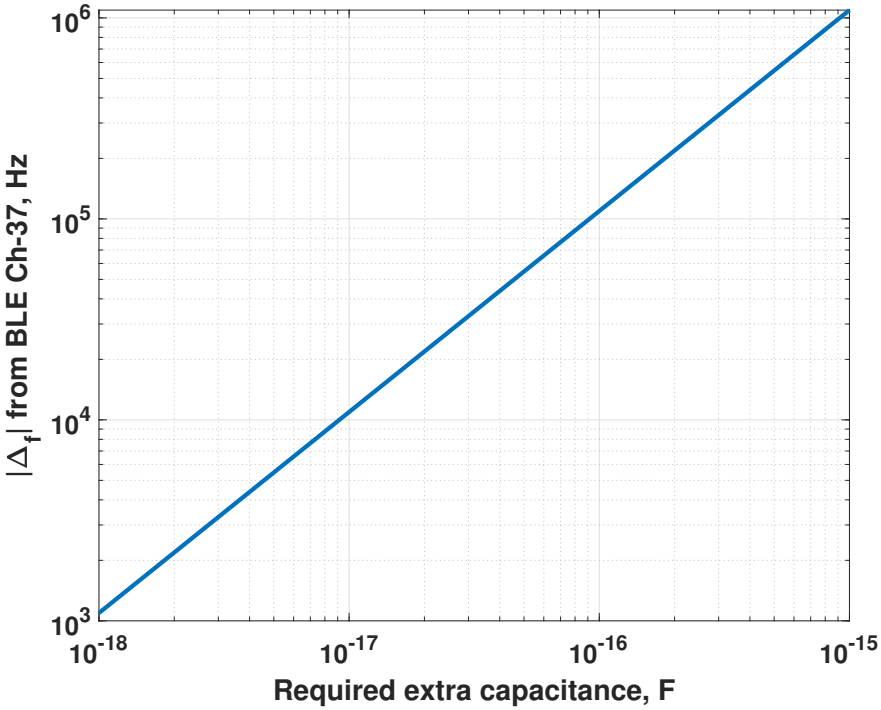

Figure 3.6. CFO versus required extra capacitance for the LC tank.

few kHz up to less than 100 kHz. The on-chip inductor for 4.8 GHz LC oscillator is set at 1 nH (Q_{PDK}=15.93) regarding its self resonance frequency (SRF) and its size. For the advertising channel 37 at 2402 MHz (VCO-Frequency=4804 MHz), the required capacitor to resonate with the 1 nH inductor is 1097.57 fF. Fig. 3.6 shows the required added capacitor to move the carrier frequency from the channel frequency. As it can be seen from Fig. 3.6, the required capacitance for few kHz of CFO can be as low as few aF which would be in the ball-park of any capacitor to p-sub parasitic cap and this would be an strong function of process variation and mismatch. Therefore, this approach is not applicable and an elegant semi-identical cap switching will be presented for kHz CFO implementation in Sec. 3.3.

3.3 Circuit Implementation

Fig. 3.7 shows the block diagram of the proposed privacy-preserving BLE/WiFi compliant Tx. To match the general architecture of a BLE/WiFi combo chip, the base-band of the design is

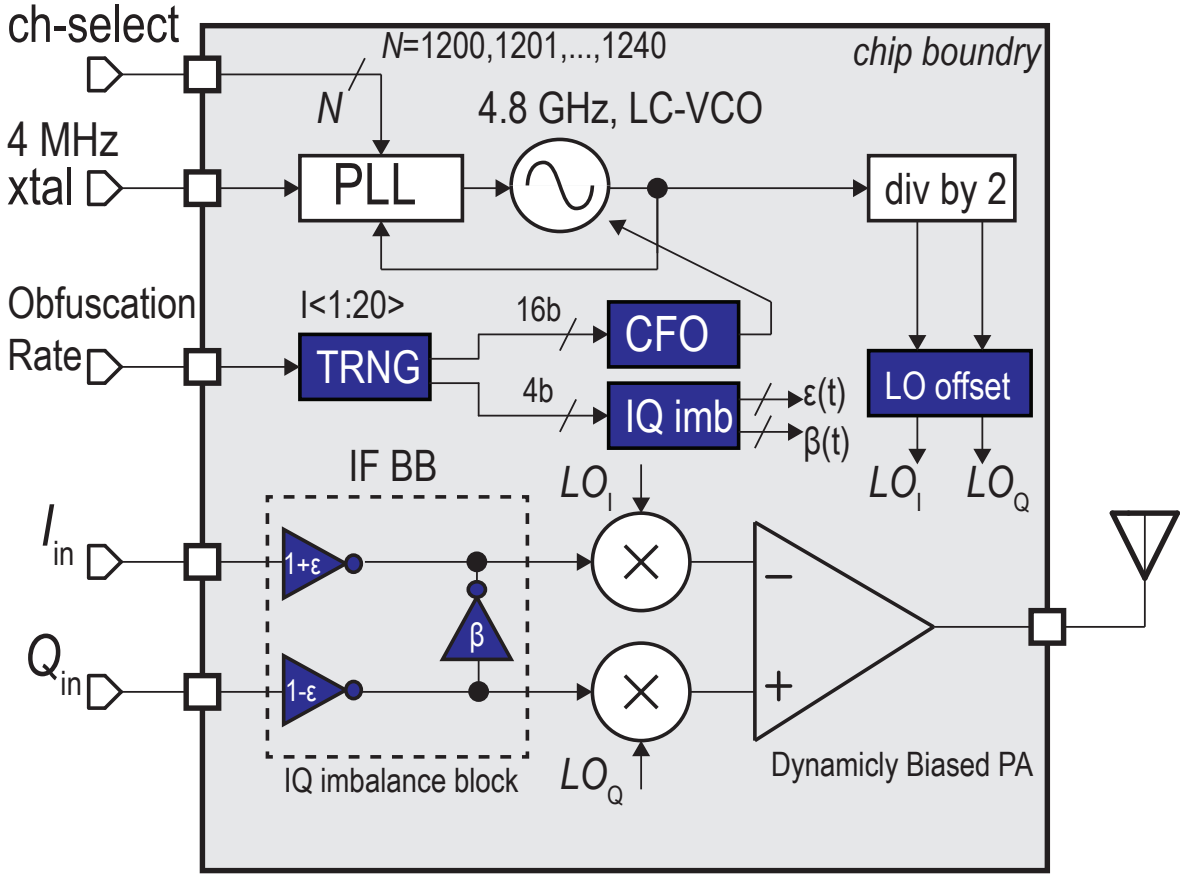

Figure 3.7. Privacy enabled WiFi/BLE Tx.

implemented by using I and Q branches to meet the required m-QAM modulation employed in WiFi, even though BLE only uses FSK modulation. An on-chip integer-N frequency synthesizer is utilized to tune a voltage controlled oscillator (VCO) to a center frequency ranging from 4800 to 4960MHz in 4MHz steps, thanks to a 4MHz crystal reference. After a divide by two circuit, in-phase and quadrature local oscillator (LO) signals are generated between 2400MHz to 2480MHz in 2MHz steps in accordance with BLE channel specifications. After locking, an additional, explicit CFO can be added during a packet transmission. The exact amount of CFO applied depends on the output of an on-chip True Random Number Generator (TRNG), which

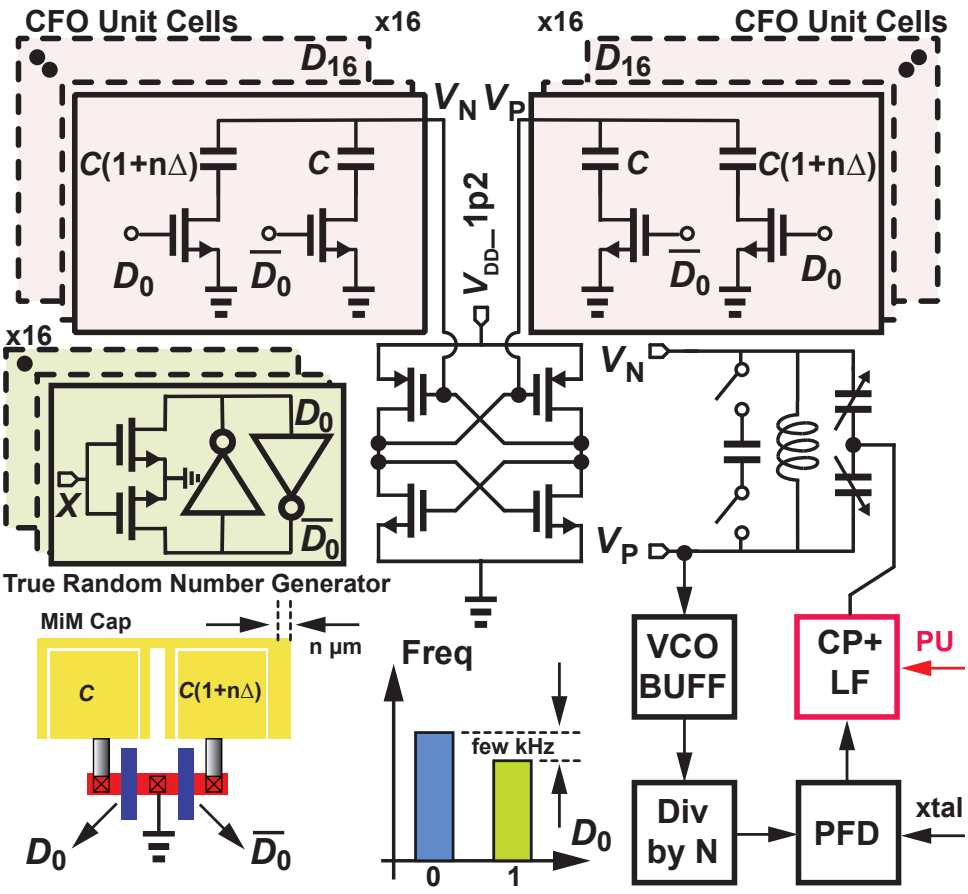

Figure 3.8. CFO implementation by using semi-identical MIM caps.

controls a 16b capacitive DAC connected to the VCO's LC tank. I/Q offset can also be added prior to distribution to the on-chip mixers, which are preceded by an I/Q imbalance generation circuit should that require eventual obfuscation as well. The output of the mixers connect to an on-chip power amplifier and then an antenna.

The BLE standard mandates that no more than $\pm$75kHz of CFO can be tolerated, which sets an upper bound for the proposed CFO circuit. Our analysis shows that for optimal CFO implementation, it requires the VCO frequency to be randomly offset around the nominal channel frequency by +/- 80kHz, which is at boundary set by the standard. To place a margin for the BLE standard, 160 kHz maximum CFO has been considered. Also, since the obfuscation effectiveness increases for lower LSB CFO values, it has been set at 1kHz. In this work, we have achieved a CFO LSB of 1kHz by toggling between two semi-identical custom MIM capacitors, as shown in

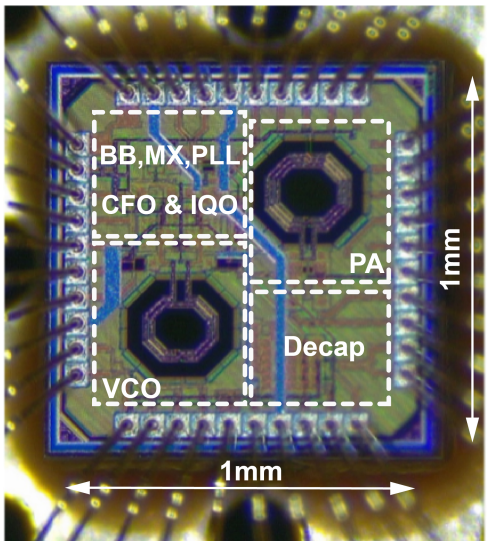

Figure 3.9. Die micrograph of the private BLE/WiFi Combo Tx.

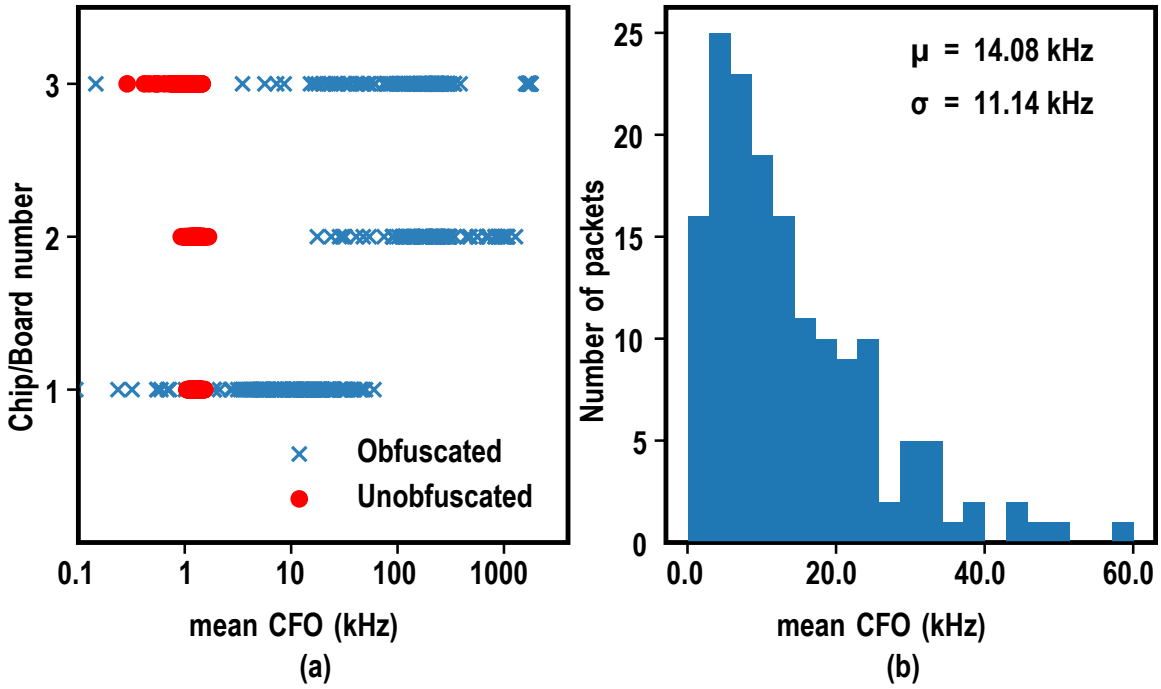

Figure 3.10. (a) Measured mean CFO across 3 chips/boards with and without the proposed obfuscation technique, and (b) TRNG enabled frequency histogram showing mean/sigma of 1.26.

Fig. 3.8. To generate very small CFO (1 kHz for advertising channel 37 at 2402 MHz, is roughly 415 ppb), semi-identical cap switching has been implemented. Adding a stripe of metal-8 to the

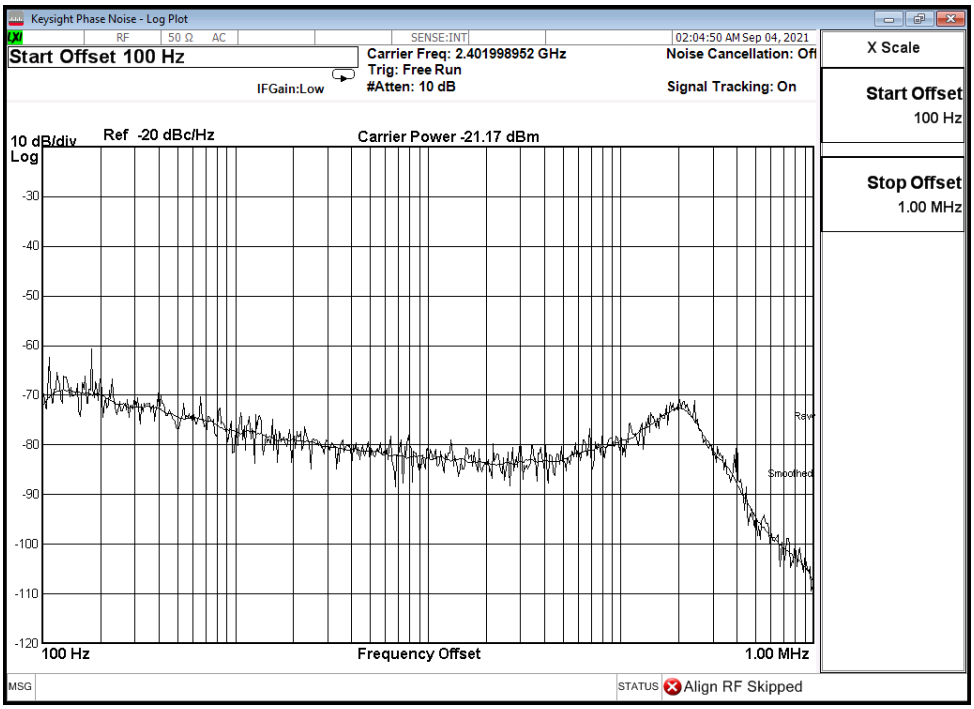

Figure 3.11. BLE advertising channel 37 phase noise.

MIM cap and doing post layout extraction, it has been optimized to achieve kHz range CFO [VG15]. A 16b Binary CDAC array is implemented alongside the 4.8 GHz LC VCO. Turning on and off every bit would result in an effective +/- ΔC seen by the tank. The ΔC should be in aF region to result in a kHz frequency offset which would require proper layout for the capacitors and their routing. The number of bits is chosen high to overcome the chip to chip variation inevitable mismatch. To achieve random CFO, an on-chip TRNG is implemented by using a back to back inverter memory cell that outputs a random bit each time the drain is pulled down using the CFO control pulse [YBS17]. Nominally, this should occur every 15 minutes to correspond with a MAC address change at the network level.

To measure the I/Q offset, the BB I/Q signals, the xtal reference of the PLL and the spectrum analyzer (MXA) should be synchronized. Knowing all the phase information, the Tx signal is captured by the MXA (sampled at 8MS/s for 1 sec) and after removing the CFO from the raw I/Q data, the baseline I/Q offset is obtained (both magnitude and its phase). Thereafter, by changing the bias level of 2.4 GHz I and Q LOs, the new set of data is captured and the I/Q

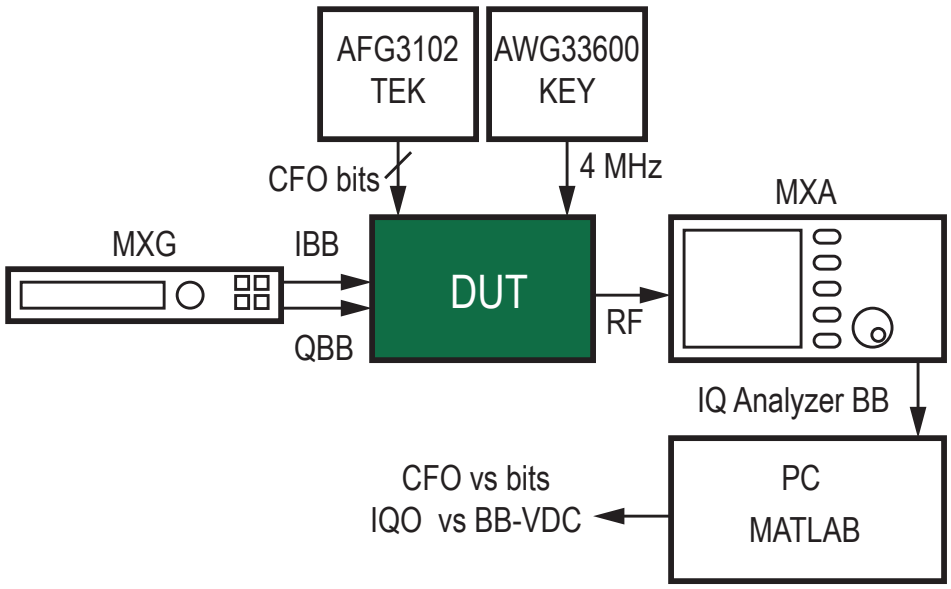

Figure 3.12. I/Q and CFO measurement setup.

offset is measured by plotting the Q versus I

3.4 Measurement Result

The fabricated private BLE/WiFi combo-chip is shown in Fig. 3.9 which occupies 1mm^2 total area and is implemented in TSMC 65nm LPCMOS process. The CFO measurement is done by changing the state of the PLL. As shown in Fig. 3.8, the PLL at the start is locked to an advertising channel, every time a packet should be sent, the PLL will turn off by powering down the charge pump and then using the on-chip CFO bits, the frequency offset will be generated. to achieve less than 1 PPM frequency offset as shown in Fig. 3.10 (measurement across 4 separate chip-on-board), frequency over time data has been captured and averaged over one BLE packet duration (400 μsec), the captured data for CFO and TRNG are shown in Fig. 3.10(a) and Fig. 3.10(b). Advertising channel 37 phase noise of the locked PLL is shown in Fig. 3.11 showing -110 dBc/Hz spot phase noise which is very much acceptable for BLE applications.

The measurement setup is shown in Fig. 3.12 in which shows that the BB is generated and fed to the DUT by MXG and then the data is captured by MXA internal receiver and processed

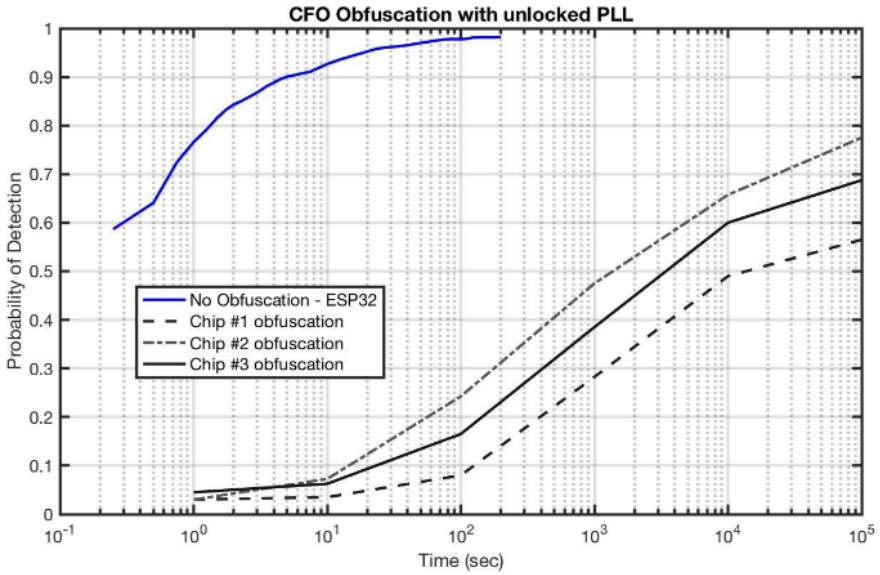

Figure 3.13. Probability of detection for commercial BLE chips and the proposed highly private Tx.

after wards.

3.5 Conclusion

With ever increasing number of BLE and WiFi enabled devices privacy of users to not being identified unwillingly will be a great matter. In this work, it has been shown that by utilizing randomization and right Tx feature, it is possible to confuse the adversary and delay user identification. Outcome of the work is shown in Fig. 3.13 which demonstrates using the proposed obfuscation methods of the proposed idea, to achieve 70% accuracy of detection over 20 devices, the user detection will be delayed from few seconds to more than 11 days. It is worth mentioning that, the CFO effect has only been shown, though utilizing the three common Tx features as CFO, IQO, and IQI, finally the user will have privacy enough not to be classified by any opposition receiving their radio signals.

3.6 Acknowledgements

Chapter 3, in part is currently being prepared for submission for publication of the material. Nikoofard, Ali; Mercier, Patrick P. The dissertation author was the primary investigator and author of this msterial.

Chapter 4

Conclusion and Suggestions

In this section, an over all conclusion of each work has been presented alongside the potential adjustments that can improve the over system performance. Regarding the 16-FSK receiver, As the target of the dissertation was to find an applicable solution for the existing problem, of long range low power high efficient radio system, using 16-FSK modulation along side the proposed semi-optimal tone filtering, proves the functionality of such approach. This should be recognized that 16-FSK better power efficiency comes at the cost of occupying more bandwidth and degrading the overall spectrum efficiency. To further improve the sensitivity alongside the power consumption of such receivers, moving to more advanced technology node can be help full. This can shrink the die area alongside with the total system power consumption. Other approaches that can be done is to enhance the system dynamic range. This can be done by inserting a low loss front-end attenuator in which does not degrade the noise figure substantially but help to adjust the signal levels within the chain not to cause the RF/IF blocks go to compression or generate inter-modulation products.

Blocker performance can also be improved by having a surface acoustic wave (SAW) filter at the front-end, accepting the increase of the noise figure and therefore drop of the sensitivity by the filters in-band loss. Moving to other ISM band frequencies is an interesting topic of research for this project. For instance, going to 2.4 GHz band, the free space path loss will increase, however the system integration would be more efficient since the antenna would be roughly

3 times smaller. On the other hand, the 433.92 MHz band, enhances the free space path loss problem, though comes at the cost of larger antenna for the system integration.

Another interesting take for implementation of the proposed would be study of using an analog to digital converter (ADC) with oversampling of the signal at the IF. This comes at the trade of between the power consumption of the ADC alongside with its noise contribution and number of bits selection not to degrade the overall system sensitivity. It should also be noted that implementation of the optimal filter within digital signal processing power consumption should be also taken into account.

Regarding the 16-FSK transmitter, the proposed test chip has shown an straight forward implementation of the 16-FSK modulated signal with modulating the low power supply voltage controlled oscillator. The overall system only includes the synthesizer for channel selection, single transistor class-E power amplifier and direct modulation technique. This approach make this design very suitable for moving to advanced technology nodes. The improvement on this work can be done on finding more efficient methods for disconnect the PLL from the VCO for channel selection and then direct modulation. Moreover, the system overall noise can be improved by adding the low drop out regulator along the band-gap reference on die.

Regarding the WiFi/BLE compliant transmitters problem, the proposed randomization of commonly studied transmitter feature has shown the ability to improve the user's privacy. This has been shows by improving the detection with high accuracy within few seconds to the same accuracy for more than a day. The elegant circuit technique of switching in and out a very similar capacitor has helped to change the VCO frequency while PLL is disconnected within few kHz that lie within the frequency inaccuracy of the commercial crystals when multiplied by N in the synthesizer. Further work in this area of hardware privacy can be done my improving the randomization and also combining multiple features of the transmitter, such as I/Q imbalance and I/Q offset. This should be mentioned that, the improvement are only acceptable while they are within the the range controlled by the standard. Moreover, methods of disconnecting and applying the obfuscation can be studied for more efficient implementation. This approach can be

generalized for all other standards that follow the same transmitter I/Q architecture.

Index

Bibliography

[AKW18] Abdullah Mohammed Alghaihab, Hun-Seok Kim, and David D. Wentzloff. Analysis of Circuit Noise and Non-Ideal Filtering Impact on Energy Detection Based Ultra-Low-Power Radios Performance. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 65(12):1924–1928, 2018.

[AMS+14] T. Abe, T. Morie, K. Satou, D. Nomasaki, S. Nakamura, Y. Horiuchi, and K. Imamura. An ultra-low-power 2-step wake-up receiver for IEEE 802.15.4g wireless sensor networks. In *2014 Symposium on VLSI Circuits Digest of Technical Papers*, pages 1–2, 2014.

[APC18] M. R. Abdelhamid, A. Paidimarri, and A. P. Chandrakasan. A −80dBm BLE-compliant, FSK wake-up receiver with system and within-bit dutycycling for scalable power and latency. In *2018 IEEE Custom Integrated Circuits Conference (CICC)*, pages 1–4, 2018.

[B. 12] B. Razavi. *RF Microelectronics*. Prentice-Hall, Upper Saddle River, NJ, USA, 2012.

[CBY+19] Xing Chen, Jacob Breiholz, Farah B. Yahya, Christopher J. Lukas, Hun-Seok Kim, Benton H. Calhoun, and David D. Wentzloff. Analysis and Design of an Ultra-Low-Power Bluetooth Low-Energy Transmitter With Ring Oscillator-Based ADPLL and 4× Frequency Edge Combiner. *IEEE Journal of Solid-State Circuits*, 54(5):1339–1350, 2019.

[FA13] Luca Fanori and Pietro Andreani. Class-D CMOS Oscillators. *IEEE Journal of Solid-State Circuits*, 48(12):3105–3119, 2013.

[IKW18] J. Im, H. Kim, and D. D. Wentzloff. A 470μW -92.5dBm OOK/FSK Receiver for IEEE 802.11 WiFi LP-WUR. In *ESSCIRC 2018 - IEEE 44th European Solid State Circuits Conference (ESSCIRC)*, pages 302–305, 2018.

[IKW19] J. Im, H. Kim, and D. D. Wentzloff. A 220- μ W -83-dBm 5.8-GHz Third-Harmonic Passive Mixer-First LP-WUR for IEEE 802.11ba. *IEEE Transactions on Microwave Theory and Techniques*, 67(7):2537–2545, 2019.

[Joh01] John G. Proakis. *Digital Communications*. McGraw-Hill, 2001.

[JWG+20] H. Jiang, P. P. Wang, L. Gao, C. Pochet, G. M. Rebeiz, D. A. Hall, and P. P. Mercier. A 22.3-nW, 4.55 cm2 Temperature-Robust Wake-Up Receiver Achieving a Sensitivity of -69.5 dBm at 9 GHz. *IEEE Journal of Solid-State Circuits*, 55(6):1530–1541, 2020.

[KBE16] V. Kopta, D. Barras, and C. C. Enz. A 420μW, 4 GHz approximate zero IF FM-UWB receiver for short-range communications. In *2016 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pages 218–221, 2016.

[KJC+19] K. Kim, E. Jeong, K. Choi, S. Kim, B. Yun, H. Jung, W. Oh, J. Ko, and S. Lee. A 915 MHz, 499 μW, –99 dBm, and 100 kbps BFSK Direct Conversion Receiver. In *ESSCIRC 2019 - IEEE 45th European Solid State Circuits Conference (ESSCIRC)*, pages 209–212, Sep. 2019.

[KM20] H. R. Kooshkaki and P. P. Mercier. A 0.55mW Fractional-N PLL with a DC-DC Powered Class-D VCO Achieving Better than -66dBc Fractional and Reference Spurs for NB-IoT. In *2020 IEEE Custom Integrated Circuits Conference (CICC)*, pages 1–4, 2020.

[LDNK18] D. Liao, F. F. Dai, B. Nauta, and E. A. M. Klumperink. A 2.4-GHz 16-Phase Sub-Sampling Fractional-N PLL With Robust Soft Loop Switching. *IEEE Journal of Solid-State Circuits*, 53(3):715–727, 2018.

[LKD+19] R. Liu, A. B. K. T., R. Dorrance, D. Dasalukunte, M. A. Santana Lopez, V. Kristem, S. Azizi, M. Park, and B. R. Carlton. An 802.11ba 495μW $-$92.6dBm-Sensitivity Blocker-Tolerant Wake-up Radio Receiver Fully Integrated with Wi-Fi Transceiver. In *2019 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pages 255–258, 2019.

[LNM20] D. Lee, A. Nikoofard, and P. P. Mercier. A -254.1-dB FoM 2.4-GHz Subsampling PLL With a -76-dBc Reference Spur by Employing a Varactor-Based Cancellation Technique. *IEEE Solid-State Circuits Letters*, 3:102–105, 2020.

[MC15] P. P. Mercier and A. P. Chandrakasan. Ultra-Low-Power Short-Range Radios. Springer International Publishing Switzerland, Springer, Cham, 2015.

[MDB+19] J. Moody, A. Dissanayake, H. Bishop, R. Lu, N. Liu, D. Duvvuri, A. Gao, D. Truesdell, N. S. Barker, S. Gong, B. H. Calhoun, and S. M. Bowers. A Highly Reconfigurable Bit-Level Duty-Cycled TRF Receiver Achieving -106-dBm Sensitivity and 33-nW Average Power Consumption. *IEEE Solid-State Circuits Letters*, 2(12):309–312, 2019.

[Mer15] Mercier, Patrick P., Chandrakasan, Anantha P. *Ultra-Low-Power Short-Range Radios*. Springer, 2015.

[MK19] V. Mangal and P. R. Kinget. Sub-nW Wake-Up Receivers With Gate-Biased Self-Mixers and Time-Encoded Signal Processing. *IEEE Journal of Solid-State Circuits*, 54(12):3513–3524, 2019.

[NPMC12] P. M. Nadeau, A. Paidimarri, P. P. Mercier, and A. P. Chandrakasan. Multi-channel 180pJ/b 2.4GHz FBAR-based receiver. In *2012 IEEE Radio Frequency Integrated Circuits Symposium*, pages 381–384, 2012.

[NZM21] Ali Nikoofard, Hamed Abbasi Zadeh, and Patrick P. Mercier. A 0.6-mW 16-FSK Receiver Achieving a Sensitivity of 103 dBm at 100 kb/s. *IEEE Journal of Solid-State Circuits*, 56(4):1299–1309, 2021.

[PGR08] N. M. Pletcher, S. Gambini, and J. M. Rabaey. A 2GHz 52 μW Wake-Up Receiver with -72dBm Sensitivity Using Uncertain-IF Architecture. In *2008 IEEE International Solid-State Circuits Conference - Digest of Technical Papers*, pages 524–633, 2008.

[PR14] J. W. Park and B. Razavi. Channel Selection at RF Using Miller Bandpass Filters. *IEEE Journal of Solid-State Circuits*, 49(12):3063–3078, 2014.

[PSO11] J. Pandey, J. Shi, and B. Otis. A 120μW MICS/ISM-band FSK receiver with a 44μW low-power mode based on injection-locking and 9x frequency multiplication. In *2011 IEEE International Solid-State Circuits Conference*, pages 460–462, 2011.

[RCS+16] N. E. Roberts, K. Craig, A. Shrivastava, S. N. Wooters, Y. Shakhsheer, B. H. Calhoun, and D. D. Wentzloff. 26.8 A 236nW -56.5dBm-sensitivity bluetooth low-energy wakeup receiver with energy harvesting in 65nm CMOS. In *2016 IEEE International Solid-State Circuits Conference (ISSCC)*, pages 450–451, 2016.

[SJDL17] H. Seok, O. Jung, A. Dissanayake, and S. Lee. A 2.4GHz, -102dBm-sensitivity, 25kb/s, 0.466mW interference resistant BFSK multi-channel sliding-IF ULP receiver. In *2017 Symposium on VLSI Circuits*, pages C70–C71, 2017.

[SLP14] N. Saputra, J. R. Long, and J. J. Pekarik. A low-power digitally controlled wideband FM transceiver. In *2014 IEEE Radio Frequency Integrated Circuits Symposium*, pages 21–24, 2014.

[Smi53] B. D. Smith. Analysis of Commutated Networks. *Transactions of the IRE Professional Group on Aeronautical and Navigational Electronics*, PGAE-10:21–26, 1953.

[SMS18] A. Sharkia, S. Mirabbasi, and S. Shekhar. A Type-I Sub-Sampling PLL With a 100×100 μm^2 Footprint and -255-dB FOM. *IEEE Journal of Solid-State Circuits*, 53(12):3553–3564, 2018.

[VG15] Christian Venerus and Ian Galton. A TDC-Free Mostly-Digital FDC-PLL Frequency Synthesizer With a 2.8-3.5 GHz DCO. *IEEE Journal of Solid-State Circuits*, 50(2):450–463, 2015.

[vvv+09] R. van Langevelde, M. van Elzakker, D. van Goor, H. Termeer, J. Moss, and A. J. Davie. An ultra-low-power 868/915 MHz RF transceiver for wireless sensor network

applications. In *2009 IEEE Radio Frequency Integrated Circuits Symposium*, pages 113–116, 2009.

[WAI20a] D. D. Wentzloff, A. Alghaihab, and J. Im. Ultra-Low Power Receivers for IoT Applications: A Review. In *2020 IEEE Custom Integrated Circuits Conference (CICC)*, pages 1–8, 2020.

[WAI20b] David D. Wentzloff, Abdullah Alghaihab, and Jaeho Im. Ultra-Low Power Receivers for IoT Applications: A Review. In *2020 IEEE Custom Integrated Circuits Conference (CICC)*, pages 1–8, 2020.

[WAI20c] David D. Wentzloff, Abdullah Alghaihab, and Jaeho Im. Ultra-low power receivers for iot applications: A review. In *2020 IEEE Custom Integrated Circuits Conference (CICC)*, pages 1–8, 2020.

[WJG+18] P. P. Wang, H. Jiang, L. Gao, P. Sen, Y. Kim, G. M. Rebeiz, P. P. Mercier, and D. A. Hall. A Near-Zero-Power Wake-Up Receiver Achieving -69-dBm Sensitivity. *IEEE Journal of Solid-State Circuits*, 53(6):1640–1652, 2018.

[WM20] P. P. Wang and P. P. Mercier. A 4.4μW -92/-90.3dBm Sensitivity Dual-Mode BLE/Wi-Fi Wake-up Receiver. In *2020 IEEE Symposium on VLSI Circuits*, pages 1–2, 2020.

[XM20] Y. Xiang and L. Milstein. Design and performance analysis for short range, very low-power communications. *IEEE Transactions on Communications*, pages 1–1, 2020.

[YBS17] Kaiyuan Yang, David Blaauw, and Dennis Sylvester. Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey. *IEEE Micro*, 37(6):72–89, 2017.

[YHW12] R. Ye, T. Horng, and J. Wu. Highly sensitive and low power injection-locked FSK receiver for short-range wireless applications. In *2012 IEEE Radio Frequency Integrated Circuits Symposium*, pages 377–380, 2012.

[YYY+19] Shiheng Yang, Jun Yin, Haidong Yi, Wei-Han Yu, Pui-In Mak, and Rui P. Martins. A 0.2-V Energy-Harvesting BLE Transmitter With a Micropower Manager Achieving 25% System Efficiency at 0-dBm Output and 5.2-nW Sleep Power in 28-nm CMOS. *IEEE Journal of Solid-State Circuits*, 54(5):1351–1362, 2019.