Arab Academy for Science, Technology and Maritime Transport

College of Engineering and Technology
Electronics and Communications

B. Sc. Final Year Project

Dual-Band Mobile Jammer

Presented By:

Abdallah Mahmoud *9104085*

Joumana Mohamed *9103405*

Mohamed Atef *9104657*

Suzy Sayed *9104250*

Supervised By:

Prof. Dr. Hesham El Badawy

July 2014

DECLARATION

We hereby certify that this material, which we now submit for assessment on the programme of study leading to the award of Bachelor of Science in Electronics and Communication Engineering is entirely our own work, that we have exercised reasonable care to ensure that the work is original, and does not to the best of our knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of our work.

Signed:

1-Abdallah Mahmoud

2-Joumana Mohamed

3-Mohamed Atef

4-Suzy Sayed

Registration No.:

1-9104085

2-9103405

3-9104657

4-9104250

Date: 7th July 7, 2014

ACKNOWLEDGMENT

First of all, we would like to thank everyone helped us along this journey from the very beginning till we achieved our final product.

Special thanks to *Prof. Hesham Elbadawy* for his ultimate assistance, whose guidance, advice, and supervision was invaluable.

We also deeply thank *Eng. Nagdy* from the NTI for his generous help and support.

Finally, we would like to thank the *Arab Academy for Science and Technology and Maritime Transport*. Their hospitality and support during the period this project took place are greatly acknowledged.

ABSTRACT

Nowadays, mobile communication has become so spread. In order that, a lot of places, organizations, or facilities require to keep quiet, on other words, some of these organizations may preserve some sort of security, so, mobile jammer has become an essential device to be used for such applications to minimize the mobile access inside different organizations or firms.

The project presents a general outline of mobile jammer instrument, giving short note about its civilian and military usage. In addition it provides insight into how the mobile jammer works. It describes the jamming techniques and gives brief explanation of the design parameters and specifications.

The report presents the system implementation design by giving general information about each section that is used in the design. It explains all electronic components used in each section in the hardware part. Also, it shows the results that have been achieved in experiments in the form of hardware and software. Finally, the report mentions some future work related to the jammers technologies.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Op-Amp	Operational Amplifier
IC	Integrated Circuit
PCB	Printed Circuit Board
DC	Direct current
AC	Alternative Current
GSM	Global System for Mobile Communication
DCS	Digital Cellular System
PCS	Personal Communication Services
RF	Radio Frequency
EMI shield	Electromagnetic Shield
BBN	Broadband Noise
BTS	Base Station Transceiver
SNR	Signal to Noise Ratio
IF	Intermediate Frequency
PC	Personal Computer
VCO	Voltage Controlled Oscillator
ADS Software	Advanced Design System Software
VSWR	Voltage Standing Wave Ratio
FR-4	Flame Retardant-4
AJ	Anti Jamming

Chapter One

1 INTRODUCTION

Presented By:-

1- *Abdallah Mahmoud*

2- *Joumana Mohamed*

3- *Mohamed Atef*

4- *Suzy Sayed*

Mobile (or cell) phones are becoming essential tools in our daily life. Needless to say, the wide use of mobile phones could create some problems as the sound of ringing becomes annoying. This could happen in some places like conference rooms, law courts, libraries, lecture rooms, masajed and in examination rooms in schools and colleges which can limit the cheating phenomenon happen there. From this point, the idea of mobile jammers appears.

A mobile jammer is an instrument used to prevent cellular phones from receiving signals from base stations. When used, the jammer effectively disables cellular phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected.

Mobile jammers were originally developed for law enforcement and military applications to interrupt communications by criminals and terrorists. [1]

Mobile phones are commonly designed to operate across several bands. In most circumstances, a jammer would also need to operate across the same bands to effectively jam mobile phones within range. The geographical range of a mobile phone jammer depends on its power level, its operating frequencies, the physical situation of the jammer, the mobile phone/s it is attempting to block, and the local environment.

Our aim in this project is to design, implement, and test a dual band mobile jammer. This jammer works at different frequencies such as: GSM 900 and DCS1800.

Chapter Two

2 CELL PHONE JAMMER

Presented By:-

1- *Abdallah Mahmoud*

2- *Joumana Mohamed*

3- *Mohamed Atef*

4- *Suzy Sayed*

2.1 THEORY OF OPERATION

As cell phones are full-duplex devices, which means they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies.

As shown in figure1, jamming devices overpower the cell phone by transmitting a signal on the same frequency and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone.

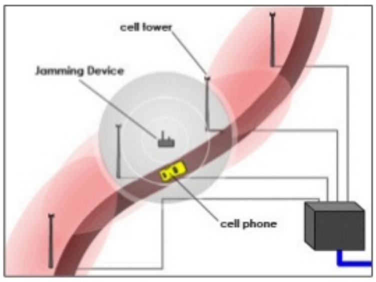


Figure 1: Cell phone jammer

To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. GSM, used in digital cellular and PCS-based systems, operates in the 900-MHz and 1800-MHz bands in Europe and Asia. [1]

2.2 CELL PHONE JAMMING LEGAL ISSUES

In the United States, United Kingdom, Australia and many other countries, blocking cell-phone services (as well as any other electronic transmissions) is against the law. In fact, the "manufacture, importation, sale or offer for sale, including advertising, of devices designed to block or jam wireless transmissions is prohibited" as well.

In most countries, it is illegal for private citizens to jam cell-phone transmission, but some countries are allowing businesses and government organizations to install jammers in areas where cell-phone use is seen as a public nuisance. In December 2004, France legalized cell-phone jammers in movie theaters, concert halls and other places with performances. France is finalizing technology that will let calls to emergency services go through. India has installed jammers in parliament and some prisons. It has been reported that universities in Italy have adopted the technology to prevent cheating. Students were taking photos of tests with their camera phones and sending them to classmates.[1]

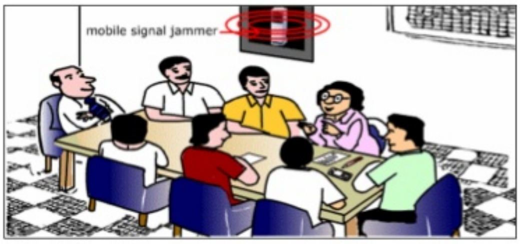


Figure 2: Mobile jammer in a meeting

2.3 JAMMING TECHNIQUES

2.3.1 Type "A" Device (Jammers)

This type of device comes equipped with several independent oscillators transmitting 'jamming signals' capable of blocking frequencies used by paging devices as well as those used by cellular/PCS systems' control channels for call establishment. When active in a designated area, such devices will (by means of RF interference) prevent all pagers and mobile phones located in that area from receiving and transmitting calls.

2.3.2 Type "B" Device (Intelligent Cellular Disablers)

Unlike jammers, Type "B" devices do not transmit an interfering signal on the control channels. The device, when located in a designated 'quiet' area, functions as a 'detector'. It has a unique identification number for communicating with the cellular base station. When a Type "B" device detects the presence of a mobile phone in the quiet room; the 'filtering' (i.e. the prevention of authorization of call establishment) is done by the software at the base station

2.3.3 Type "C" Device (Intelligent Beacon Disablers)

Unlike jammers, Type "C" devices do not transmit an interfering signal on the control channels. The device, when located in a designated 'quiet' area, functions as a 'beacon' and any compatible terminal is instructed to disable its ringer or disable its operation, while within the coverage area of the beacon. Only terminals which have a compatible

4

receiver would respond and this would typically be built on a separate technology from cellular/PCS e.g., cordless wireless, paging, Bluetooth, …. On leaving the coverage area of the beacon, the handset must re-enable its normal function.

2.3.4 Type "D" Device (Direct Receive & Transmit Jammers)

This jammer behaves like a small, independent and portable base station, which can directly interact intelligently or unintelligently with the operation of the local mobile phone. The jammer is predominantly in receiving mode and will intelligently choose to interact and block the cell phone directly if it is within close proximity of the jammer.

2.3.5 Type "E" Device (EMI Shield - Passive Jamming)

This technique is using EMI suppression techniques to make a room into what is called a Faraday cage. Although labor intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage – or in this case a target room. [2]

Then we can conclude all these types with the below table indicating the status of each type **as shown in table 1**

Table 1: Comparison between different jamming techniques

Type	Emergency calls	Efficiency	Regularity Approval	Implementation
A	Blocked	Low	Not allowed	Very simple
B	Allowed	Medium	Required	Complex (required third party)
C	Allowed	High	Required	Complex (required intelligent handset)
D	Allowed	Medium	Required	Simple
E	Blocked	High (no signal transmitted)	Allowed	Simple

Chapter Three

3 DESIGN PARAMETERS & SPECIFICATIONS

Presented By:-

1- Abdallah Mahmoud

2- Joumana Mohamed

3- Mohamed Atef

4- Suzy Sayed

3.1 NOISE JAMMING

For *noise jamming*, the jamming carrier signal is modulated with random noise waveform. The intent is to disrupt the AJ communication waveform by inserting the noise into the receiver. The bandwidth of the signal can be as wide as the entire spectrum width used by the AJ system or much narrower, occupying only a single channel

- **Broadband Noise Jamming**

Broadband noise (BBN) jamming places noise energy across the entire width of the frequency spectrum used by the target radios. It is also called *full band* jamming and is sometimes called barrage jamming. This type of jamming is useful against all forms of AJ communications.

This type of jamming essentially raises the background (thermal) noise level at the receiver, creating a higher noise environment for the AJ system. Noise is the nemesis for any communication system, and if the noise level can be increased it makes it more difficult for the communication system to operate. [3]

3.2 FREQUENCY BAND

The basic purpose of a GSM Mobile Jammer is to block or hinder communication between the Base Transceiver Station and the Mobile Station. This can only be achieved by rendering the transmission between them incomprehensible. The basic technique for accomplishing this goal is to create disturbance on the GSM transmission frequencies.
In our project we want to jam on both GSM 900 and GSM 1800 (DCS) so, we want to know the uplink and downlink frequencies for both of them and this was **shown in table2**

Table 2: Operating frequency band

	UPLINK (Handset transmit)	DOWNLINK (Handset receive)	USED IN EGYPT BY:
GSM 900	890-915 MHz	935-960 MHz	**Vodafone- Mobinil**
DCS 1800	1710-1785 MHz	1805-1880 MHz	**Vodafone- Mobinil- Etisalat**

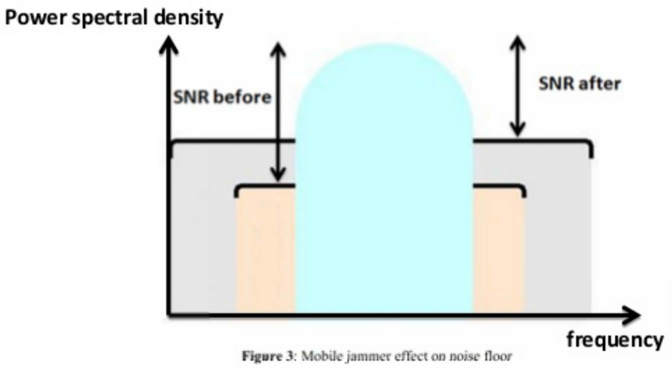


Figure 3: Mobile jammer effect on noise floor

The problem with jamming the entire band or the uplink frequencies is that we are aiming to disrupt communication at the BTS. For this we need a very high power transmitter that will create a powerful signal strong enough to reach the BTS. Furthermore, this action will cause the Signal to Noise ratio at the BTS to fall which will, in effect, cause all incoming signals at the BTS to be corrupted. Thus all incoming connections to the BTS will be disturbed which will jam the Mobile Stations throughout the entire coverage region of the BTS i.e. its cell. In contrast, if we create disturbance over the Downlink frequencies, we only need a transmitter powerful enough to create a signal that disrupts communication in our required area. This causes only the Mobile Stations in the specific area to be jammed and leaves the ones outside it alone. Summing it all up, we get the following result:

- Jamming the uplink or entire band requires a high power transmitter and disrupts communication over an entire cell
- Jamming the downlink band requires a transmitter of sufficient power to jam the required area only and does not disturb the communication outside it.[4]

Therefore, our goal is to disrupt communication over downlink frequencies only.

3.3 JAMMING ZONE

This parameter is very important in our design, since the amount of the output power of the jammer depends on the area that we need to jam.

Our design is established upon $D = 10\ meters$ for DCS 1800 band and $D = 20\ meters$ for GSM 900 band.

3.4 FREE SPACE LOSS

It is the loss in signal strength of an electromagnetic wave that would result from a line-of-sight path through free space.

Free space path loss could be calculated through **eq.1**

$$L_{FSP} = 32.45 + 20logD + 20logF \ \ (dB) \qquad (1)$$

Where, $D\ in\ Km\ and\ F\ in\ MHz$

The maximum free space loss (worst case F) happens when the maximum frequency is used in **eq.1**. Using 1880 MHz and D=10 meters gives:

$$MAX\ L_{FSP} = 32.45 + 20log\ (0.01)\ + 20log\ (1880)\ = \mathbf{58\ dB}$$

3.5 JAMMING TO SIGNAL RATIO (J/S)

Jamming is successful when the jamming signal denies the usability of the communication transmission. Usually, a successful jamming attack requires that the jammer power is roughly equal to signal power at the receiver (mobile device).

The general equation of the jamming-to-signal ratio is given as follows in **eq.2**

$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j} \quad (2)$$

Where:

P_j=Jammer Power

G_{jr}= Antenna Gain from Jammer to Receiver

G_{rj}=Antenna Gain from Receiver to Jammer

R_{tr}=Range between Communication Transmitter and Receiver

B_r=Communication Receiver Bandwidth

L_r =Communication Signal Loss

P_t=Transmitter Power

G_{tr}= Antenna Gain from Transmitter to Receiver

G_{rt}=Antenna Gain from Receiver to Transmitter

R_{jr}=Range between Jammer and Communication Receiver

B_j=Jammer Bandwidth

L_j=Jamming Signal Loss.

So the SNR of the jammer in eq.3

$$SNR = \frac{S}{J} \quad (3)$$

Where S=mobile station signal power receiver and J= jammer power at mobile receiver.
And the $S_{Max} = -15\text{dBm}$ For GSM, the specified $SNR_{Min} = 9\text{ dB}$

This will be used as the worst case scenario of the jammer in order to have maximum jamming power

This could be clearly clarified **in figure 3:**

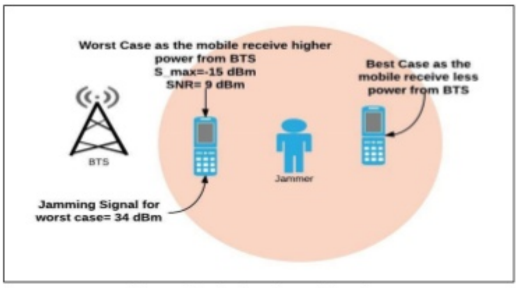


Figure 4: Best and worst case of jamming

This figure shows the best and the worst case according to jamming point of view.

As we have a mobile **near to the base station** (worst case) we can conclude that this mobile received a high power from the base station so if we want to jam this one, we should have **a high power of jamming** to overflow its received power.

In contrast, if we have a mobile **further from the base station** it will receive a power much lower than the previous case and this will be best case for jamming as it **does not need high power** to jam.

10

3.6 POWER CALCULATIONS

Here in this part, we want to calculate the needed power in order to jam a cell phone within a distance of 10 m for DCS and 20 m for GSM 900 , from the above considerations we shall calculate for the worst case ($SNR_{min} = 9dB$, $S_{max} = -15dBm$) in order to be sure we will have a jamming in everywhere as in **eq.4**

$$J_r \text{ (jammer power at mobile receiver)} >= S_{max} - SNR_{min} \quad (4)$$

Therefore,

$$J_r >= -24dBm$$

Taking into account the free space loss as we calculate it before in **eq.1** and substitute in **eq.5**

$$Jammer\ output\ power = J_r + L_{FSP} \quad (5)$$

Therefore,

$$Output\ Power = -24 + 58 = 34dBm$$

So, this power will be needed for the worst case for jamming the specified region.

Chapter Four

4 SYSTEM IMPLEMENTATION

Presented By:-

1- Abdallah Mahmoud

2- Joumana Mohamed

3- Mohamed Atef

4- Suzy Sayed

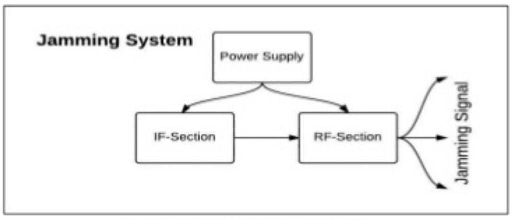


Figure 5: Jamming system block diagram

4.1 POWER SUPPLY

It is used to supply both sections IF and RF with their suitable voltages. Any power supply consists of the following main parts:

i. **Transformer**: - is used to transform the 220VAC to other levels of voltages
ii. **Rectification**: this part is to convert the AC voltage to a DC. We have two methods for rectifications:

a. **Half wave-rectification**: the output voltage appears only during positive cycles of the input signal.
b. **Full wave –rectification**: a rectified output voltage occurs during both the positive and negative cycles of the input signal.

iii. **The Filter**: used to eliminate the fluctuations in the output of the full wave rectifier

iv. **Regulator**: this is used to provide a desired DC-voltage

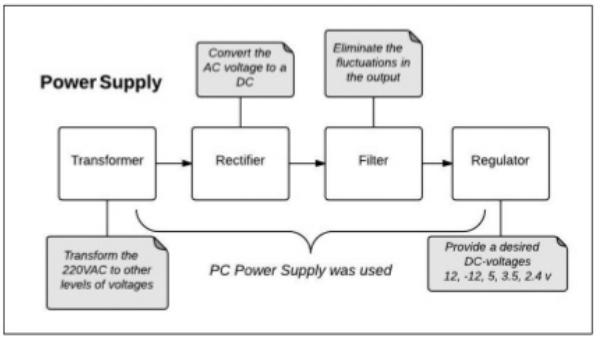


Figure 6: Power Supply block diagram

Our aim is to get +12, -12, 5, 3.5 and 2.4 volts in our design. We can get all values direct from PC power supply except 2.4 volt, this value we can get from regulator circuit.
The regulator circuit consists of:

1) LM317 Regulator
2) Two resistors
3) Two capacitors

Our equation of variable regulator as in **eq.6**

$$V = 1.25\left(1 + \frac{R_2}{R_1}\right) \tag{6}$$

Where R_1 and R_2 are selected according to our required voltages.
In our design of the regulator circuit we have first the LM317 regulator which consists of: Input, output, and adjustment pins **as shown in the below figure 6:**

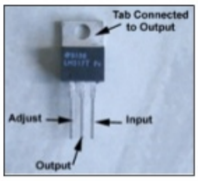


Figure 7: LM317 regulator

Then, we connect this IC with two resistors to get the desired voltage, and connect two capacitors one at the input and the other at the output of the regulator used for the stability of the regulator's control loop [6] **as shown in the circuit of figure 7**:

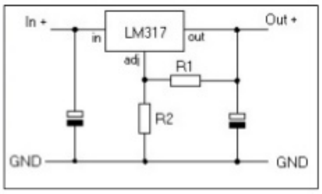


Figure 8: Regulator circuit

In order to calculate the 2.4 volt we have to select two resistors to give the required voltage.
Put $R_1 = 160\,\Omega$ and $R_2 = 148\,\Omega$ and substitute in the above equation we will get $V = 2.406\ volt$, then take this voltage from the output pin.

4.2 INTERMEDIATE FREQUENCY (IF) SECTION

An **intermediate frequency (IF)** is a frequency to which a carrier is shifted as an intermediate step in transmission or reception.

The IF Section is the section which generates the tuning voltage for the VCO in the RF Section so that the output of the VCO is swept through the desired range of frequencies. The output of the IF Section is triangular wave of frequency 10KHz to which noise is added and then the signal is offset by a certain DC value to obtain the required tuning voltage.

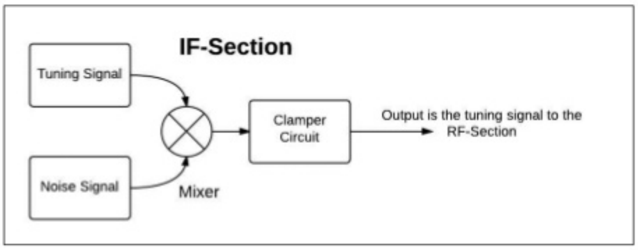


Figure 9: IF Section block diagram

The components of the IF Section are as follows:

Table 3: IF Section components

Triangular Wave Generator	555 Timer IC
Noise Generator	Zener Diode
Signal Mixer	OpAmp in Summing configuration
Offset Circuit	Diode Clamper

4.2.1 Triangular Wave Generator

The main use of the triangular wave is to **sweep the VCO** through the desired frequency range.

In the design, we shall use 555timer IC operating in the astable mode to generate the sweeping signal.

First, the output frequency and voltage depends on the charging and discharging of the capacitor and resistor values .The voltage depends on power supply for the IC as frequency is independent of the supply voltage.

To determine the output sweeping voltage

$$V_{TH} = \frac{2}{3}V_{cc} \qquad V_{TL} = \frac{1}{3}V_{cc}$$

So the output voltage will swing between $\frac{1}{3}V_{CC}$ $and \frac{2}{3} V_{CC}$

To determine the output frequency:

The charge time (T_H) is given by **eq.7**

$$T_H = 0.693\,(R_A + R_B) * C \qquad (7)$$

The discharge time (T_L) is given by **eq.8**

$$T_L = 0.693 * R_B * C \qquad (8)$$

By sub **eq.7 & eq.8** to get the total period (T) in **eq.9**

$$T = T_H + T_L = 0.693(R_A + 2 * R_B) * C \qquad (9)$$

The frequency of oscillation (F) is given in **eq.10**

$$F = \frac{1}{T} = \frac{1.44}{(R_A+2R_B)C} \qquad (10)$$

16

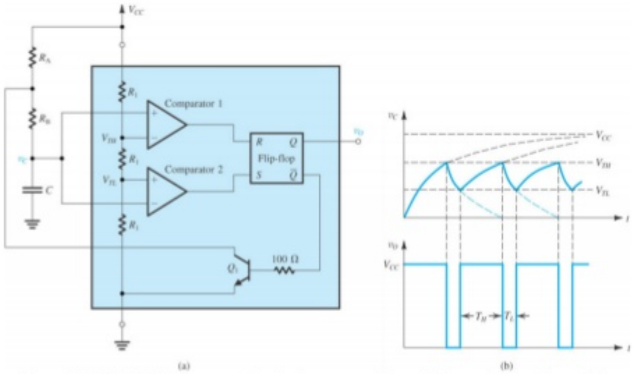


Figure 10: (a) The 555 timer connected to implement an astable multivibrator. (b) Waveforms of the circuit in (a).

The duty cycle (D) is determined using **eq.11**

$$D = \frac{R_B}{R_A + 2R_B} \qquad (11)$$

In this case the duty cycle will always be greater than 50%.[5]

In our project we need the duty cycle to be 50% so that the charging time equals the discharging time. This can be achieved by **eq.12**

- Using $R_A = R_B$
- Placing diode across R_B

$$F = \frac{1.44}{C(R_A + R_B)} \qquad (12)$$

In our design:

Table 4: Design calculations

$R_A = R_B = 750\Omega$	$C = 0.1\mu F$	$V_{CC} = 12$ volt
$F = 9.6$ kHz	Output voltage will swing between 4 to 8 v	

Using OrCAD simulation:

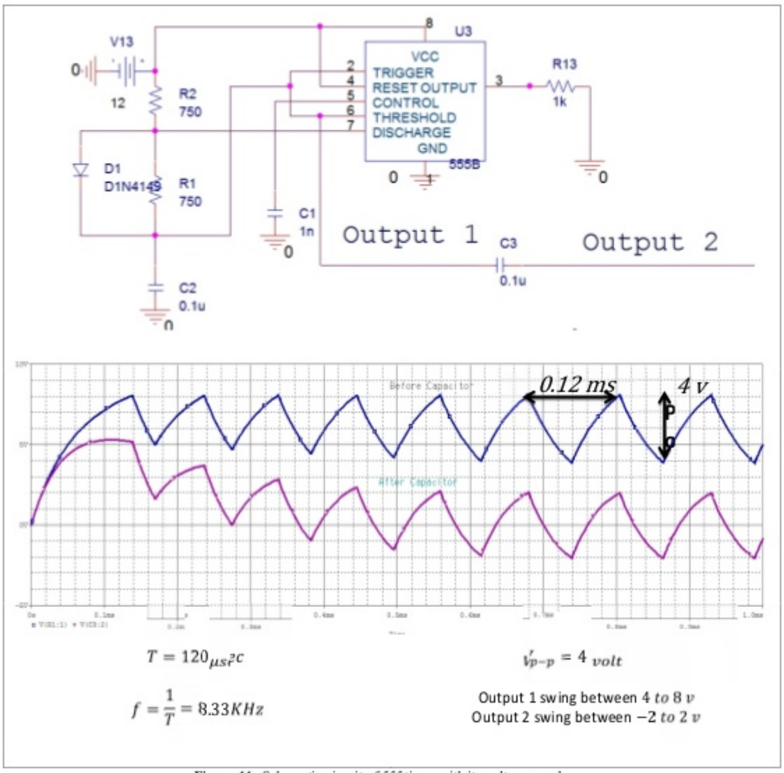


Figure 11: Schematic circuit of 555 timer with its voltage graph

As shown in figure 11, a coupling capacitor was added to the output of 555timer. A coupling capacitor is used to connect between two circuits. It only passes the AC signal and blocks the DC signal.[6]

Hardware results:

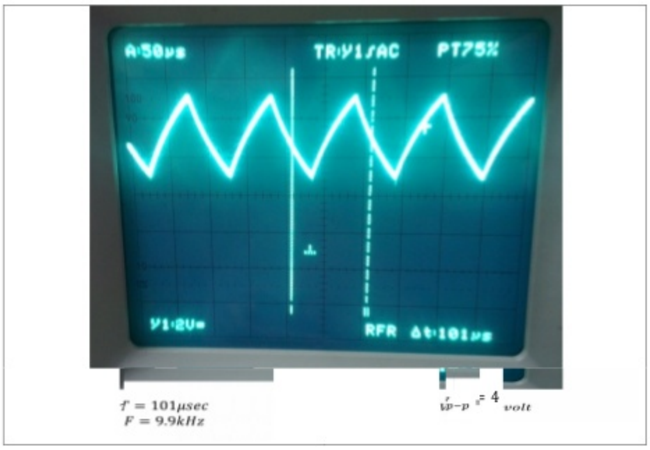


Figure 12: The output signal of 555timer on the oscilloscope

Figure 12 shows the actual obtained signal on the oscilloscope. It satisfies the desired goals of the designed triangular wave generator subsection. Hereby, we move to another section.

4.2.2 Noise Generator

In this project the jamming system needs a certain type of noise to cover a portion band of spectrum, so the most applicable type of noise in this case is the **white noise**. The noise in general can be defined as a Random movement of charges or charge carriers in an electronic device generates current and voltage that vary randomly with time.

White noise is a random signal (or process) with a flat power spectral density. In other words, the signal's power spectral density has equal power in any band, at any centre frequency, having a given bandwidth. White noise is considered analogous to white light which contains all frequencies. An infinite bandwidth, white noise signal is purely a

theoretical construction. By having power at all frequencies, the total power of such a signal is infinite.

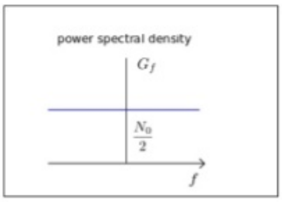


Figure 13: Ideal white noise power spectral density

In practice, a signal can be "white" with a flat spectrum over a defined frequency band.

Our noise generator is based on the phenomenon of avalanche noise generated by operating a **Zener diode** in its **reverse breakdown region**.

Operating in the reverse mode causes what is called avalanche effect, which causes **wide band noise**.

The noise generator circuit consists of a 6.8 V Zener diode with a small reverse Current.

This noise is then amplified and used in our system. We use two amplification stages:

- First stage, we use NPN transistor as common emitter
- Second stage, we use the LM386 IC. [4]

Circuit used

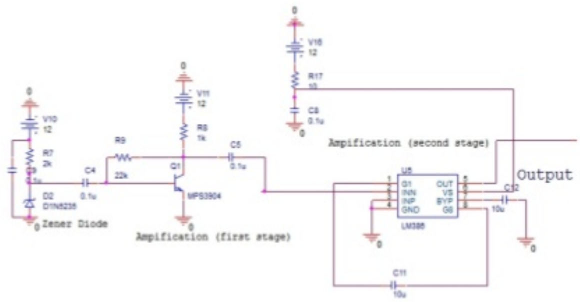


Figure 14: Schematic diagram of the noise generator in IF section

Spectrum analyzer output:

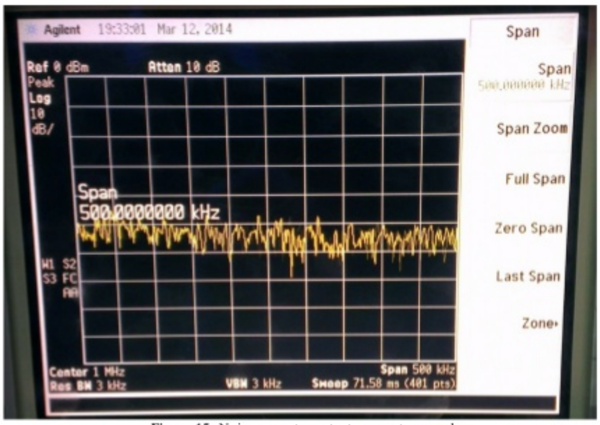


Figure 15: Noise generator output on spectrum analyzer

From the results shown in figure 15 we see that the implemented noise generator satisfies the desired functionality. So, we can successfully continue the jamming design process.

4.2.3 Mixer

Mixer is a nonlinear circuit that combines two signals in such away to produce the sum and difference of the two input frequencies at the output.

The mixer here is just an amplifier that operates as a summer. So, the noise and triangular wave will be added together before entering the VCO. The LM741 IC was used to achieve this.

We need to amplify the noise signal so we took $R_2 = 1\ k\Omega$ and we need the tuning signal to have the same ratio so we took $R_1 = 2\ k\Omega$

21

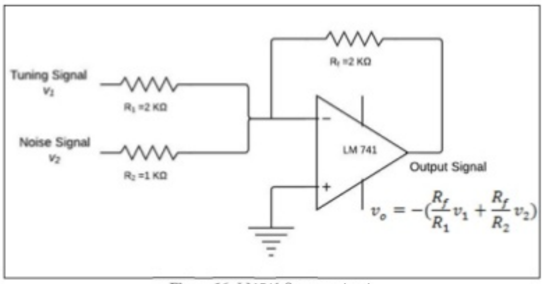


Figure 16: LM741 Summer circuit

The output signal as in **eq.13**

$$v_o = -(v_1 + 2 * v_2) \quad (13)$$

Hardware results:

Figure 17: The hardware results of the mixer circuit on the oscilloscope

As figure 17 shows the stability of the mixer circuit which contribute to continue our design in the same manner.

4.2.4 Clamper

A clamping circuit is used to place either the positive or negative peak of a signal at a desired level. The dc component is simply added or subtracted to/from the input signal.

The circuit will be called a positive clamper, when the signal is pushed upward by the circuit. When the signal moves upward, as shown in figure 17, the negative peak of the signal coincides with the zero level.

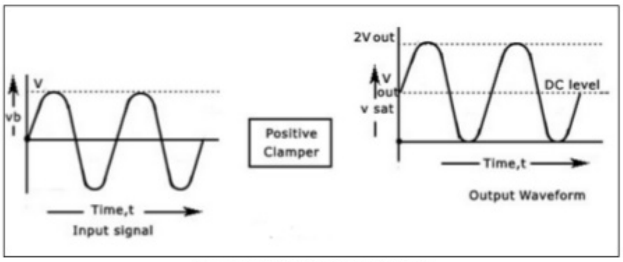


Figure 18: Positive clamper illustration

The input of the VCO must be bounded from 0 to 4 V to get the needed frequency range. So, we need to add a positive clamper circuit to get our goal (as the output from the 555timer had a DCoffset).

The clamper consists of a capacitor connected in series with a resistor and diode.

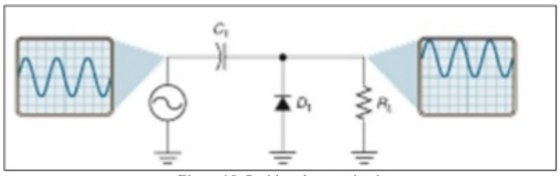


Figure 19: Positive clamper circuit

- The shape of the waveform will be the same, but its level is shifted either upward or downward
- There will be no change in the peak-to-peak value of the waveform due to the clamping circuit.
- There will be a change in the peak and average values of the waveform.
- The values for the resistor R and capacitor C should be determined from the time constant equation of the circuit, t = RC. The values must be large enough to make sure that the voltage across the capacitor C does not change significantly during the time interval the diode is non-conducting. In a good clamper circuit, the circuit time constant t = RC should be at least **ten times** the time period of the input signal voltage.[7]

So we took the value of $C = 0.1\mu F, R = 100k\Omega\ ,\ T = RC = 0.01sec = 10msec$

$$T_{signal} = 100\mu sec$$
$$\frac{T}{T_{signal}} = 100$$

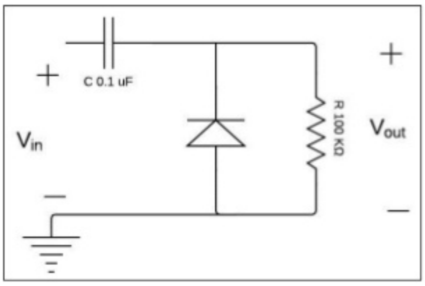


Figure 20: Clamper circuit design

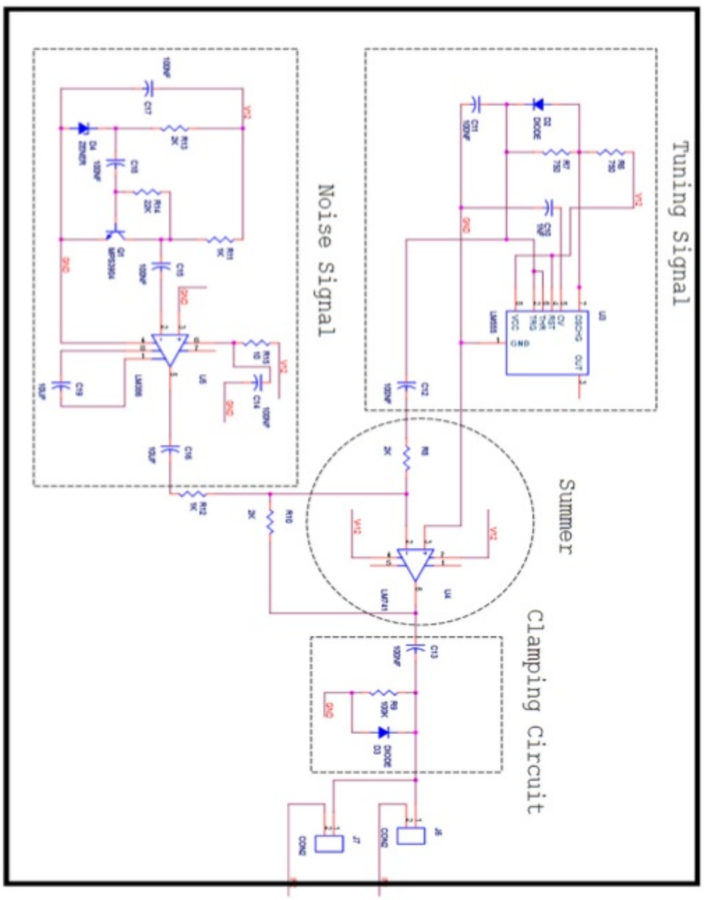


Figure 21: IF Section complete schematic diagram

4.3 RADIO FREQUENCY (RF) SECTION

Radio frequency (RF) is a rate of oscillation in the range of around 3 kHz to 300 GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals.

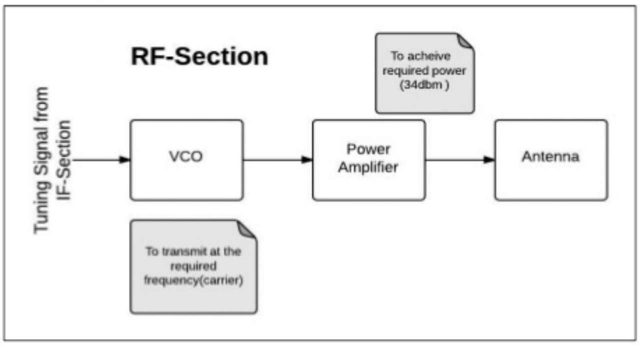


Figure 22: RF Section block diagram

This is the most important part of the Jammer.

The components of the RF Section are as follows:

Table 5: RF Section components

Voltage Controlled Oscillator	Crystek VCO
Power Amplifier	Hitachi PF08109B
Antenna	Omni-directional antenna

The selection of these components was based on the specification of the jammer such as

- Desired frequency range
- Coverage area

All the components used have 50 Ω output impedance, so a 50 Ω microstrip was used for component matching. The width of the microstrip was calculated using the Advanced Design System (ADS) LineCalc.

4.3.1 Voltage Controlled Oscillator

A **voltage-controlled oscillator** or **VCO** is an electronic oscillator whose oscillation frequency is controlled by a voltage input. The applied input voltage determines the instantaneous oscillation frequency.

It is the heart of the RF-section. It is the device that generates the carrier for the noise signal which will interfere with the cell phone.

The output of the VCO has a frequency which is proportional to the input voltage, thus, we can control the output frequency by changing the input voltage. When the input voltage is DC, the output is a specific frequency, while if the input is a triangular waveform, the output will span a specific frequency range. So we choose to have a tunable VCO to sweep over the range of frequencies and cover the whole band.

In our design, we need to find a VCO for GSM 900 and DCS 1800. There are three selection criteria for selecting a VCO for this application

- It should cover the bands that we need.
- It should run at low power consumption.

Moreover, we need to minimize the size of GSM-jammer. So, we started to search through the internet for VCO's that work for GSM 900 & GSM 1800 bands.

We found the following VCO IC's

Table 6: VCO Specifications

CVC055CL	**CVC055BE**
GSM 900	DCS 1800
Output frequency is 830-970MHz	Output frequency is 1785-1900MHz
Tuning Voltage=0.5 to 4.5 v	Tuning Voltage=0.3 to 4.7 v
Output power is up to 7dBm	Output power is up to 5dBm
	

VCO Tuning Curve

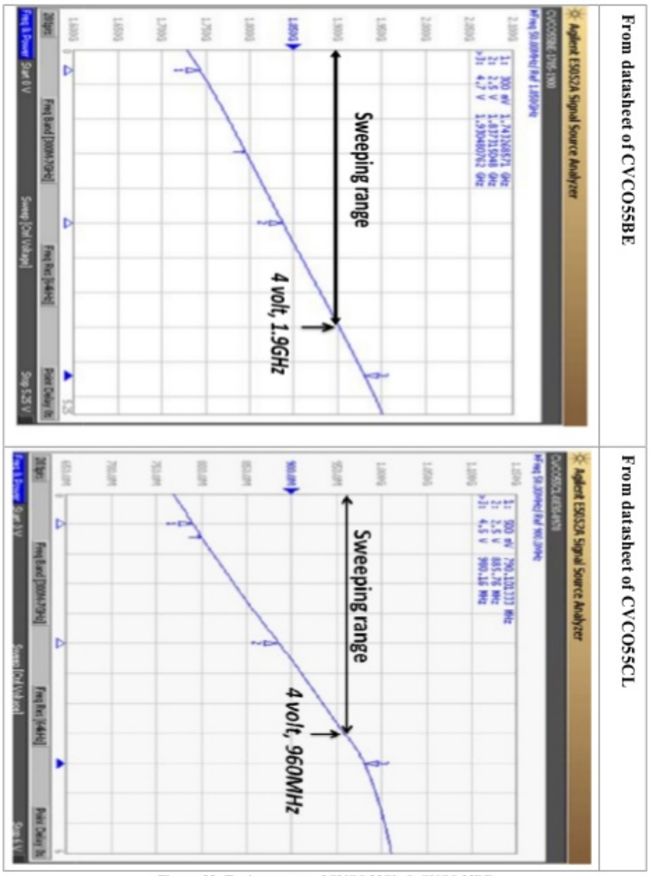


Figure 23: Tuning curves of CVCO55CL & CVCO55BE

We choose the ICs of all the design for the following reasons:

- Surface mount, which reduces the size of product.
- Having large output power that reduces the number of amplification stages that we need.
- Having same value of power supply which is typically equal to 5 volt.
- Having same noise properties.

4.3.2 Power Amplifier

An **RF power amplifier** is a type of electronic amplifier used to convert a low-power radio-frequency signal into a larger signal of significant power, typically for driving the antenna of a transmitter. Since 5dBm output power from the VCO does not achieve the desired output power of the GSM jammer, we had to add an amplifier with a suitable gain to increase the VCO output to 34dBm.

Figure 24: PF08109B IC

Power amplifier requirements

1. Output power should be around 34dBm
2. Operating frequency in the specified band

We found the power amplifier PF08109B meets our requirements and available in an old nokia mobile phones.

The PF08109B

- Has high gain of 35dB. As datasheets illustrated that this IC
- Is designed to work in dual band GSM & DCS

Output power relation with frequency from the datasheet for both GSM and DCS

For GSM

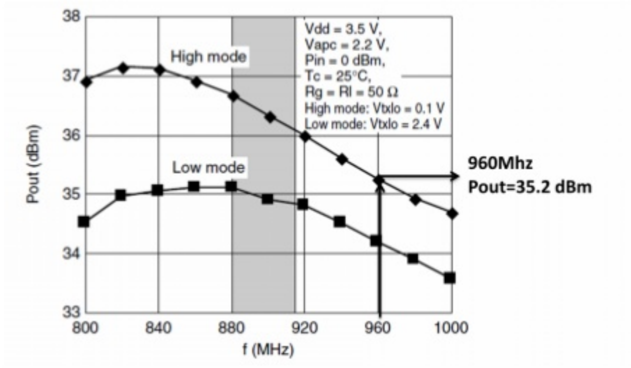


Figure 25: The output power vs. frequency curve of the PF08109B in GSM

For DCS

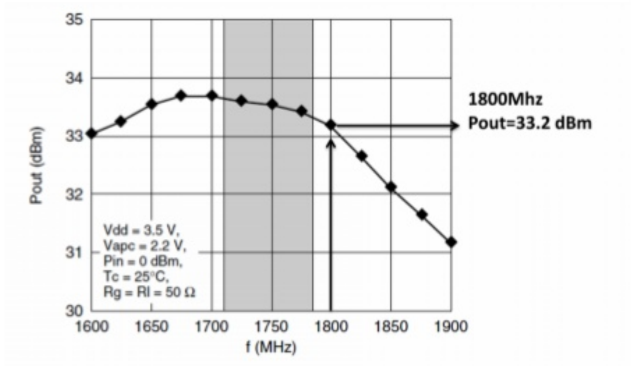


Figure 26: The output power vs. frequency curve of the PF08109B in DCS

30

Power amplifier gain from the datasheet for both GSM and DCS

For GSM

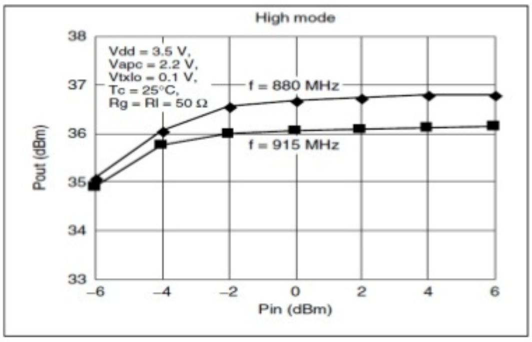


Figure 27: Input power vs. output power curve in PF08109B for GSM

For DCS

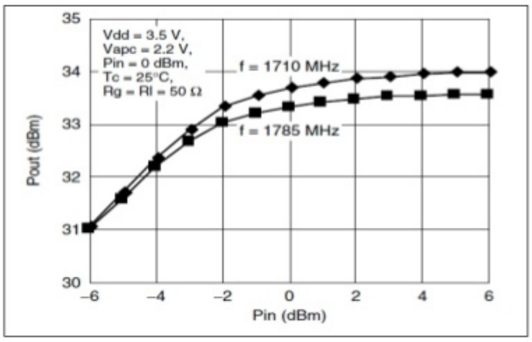


Figure 28: Input power vs. output power curve in PF08109B for DCS

31

4.3.3 Antenna

A proper antenna is necessary to transmit the jamming signal. In order to have optimal power transfer, the antenna system must be matched to the transmission system. In this project, we used two 1/4 wavelength monopole antennas, with 50 Ω input impedance so that the antennas are matched to the system. We used monopole antenna since the radiation pattern is omni-directional.[8]

Antenna Specifications

Table 7: Antenna Specifications

The GSM Antenna	The DCS Antenna
Frequency: 850MHz-1GHz	Frequency: 1700-1900MHz
Input impedance 50	
[illegible]	
	

We used dual band antenna for both GSM and DCS.

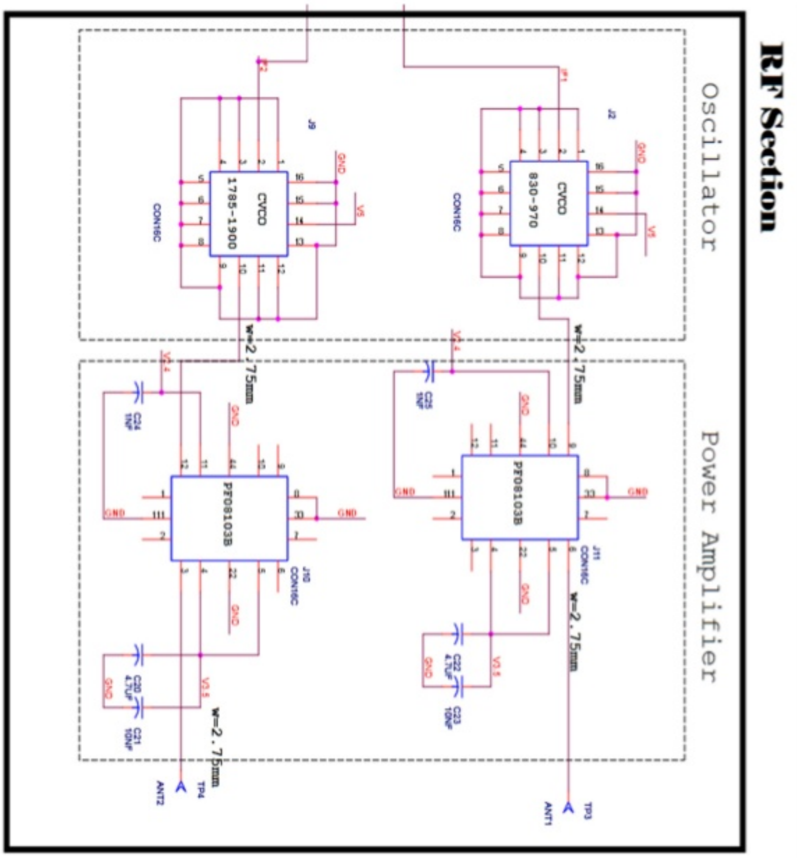
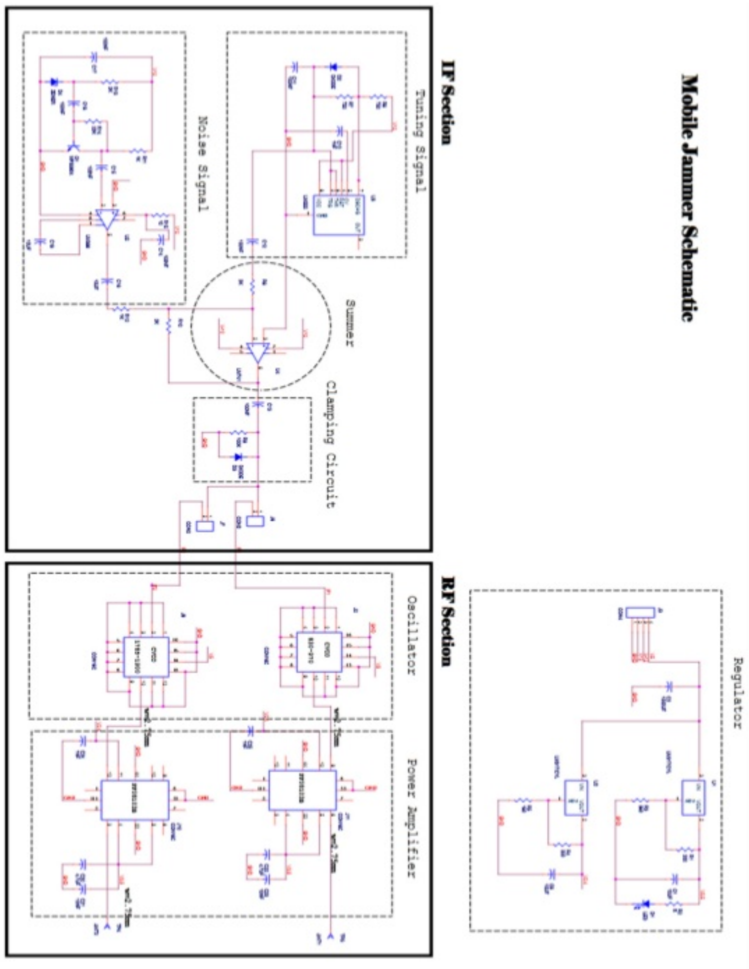


Figure 29: RF section complete schematic diagram



34

Figure 30: Jammer complete schematic diagram

Chapter Five

5 RESULTS & ANALYSIS

Presented By:-

1- *Abdallah Mahmoud*
2- *Joumana Mohamed*
3- *Mohamed Atef*
4- *Suzy Sayed*

After we completed the implementation of our circuit and got the hardware results, we have to declare some important points:

- The implementation of our PCB is completed by using FR-4 substrate with two layers.
- We needed to calculate the width of the transmission line in RF section in order for the circuit to work properly and match the components impedance (50Ω). [9] For that, we used ADS software, LineCalc feature, to calculate the width which was equal to 2.72 mm.
- After the hardware was implemented, we noticed that the power amplifier in the RF section is overheated during the circuit operation. So, it was supposed to place a heat sink underneath it to avoid that.
- We got the RF components from 'Mouser' company in US, as they are not available in local market. Meanwhile, the IF components were all available in local market.
- We were not able to simulate the RF section's results, as the components' libraries were not available in any CAD tool.

- We noticed in the hardware implementation testing that the jamming distance changed from that of the analytical computed one. We calculated the distance for GSM worst case scenario using the maximum frequency of the targeted band as well. As the power received from the BTS decrease, the jamming distance would increase. So, in real life, we expect the jamming distance would increase to more than 20 m for GSM.

PCB Layout

Top Layer

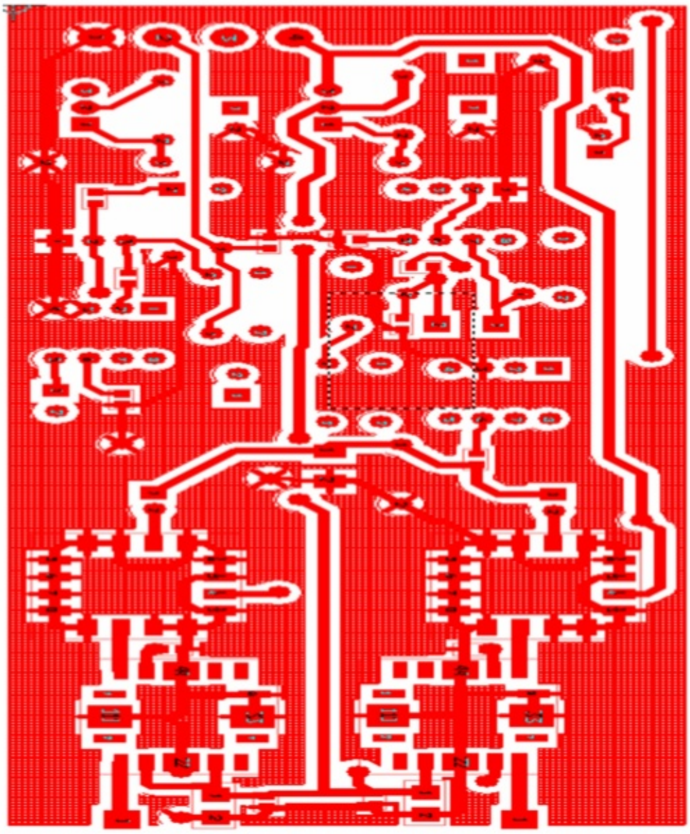


Figure 31: PCB top layer layout

Bottom Layer

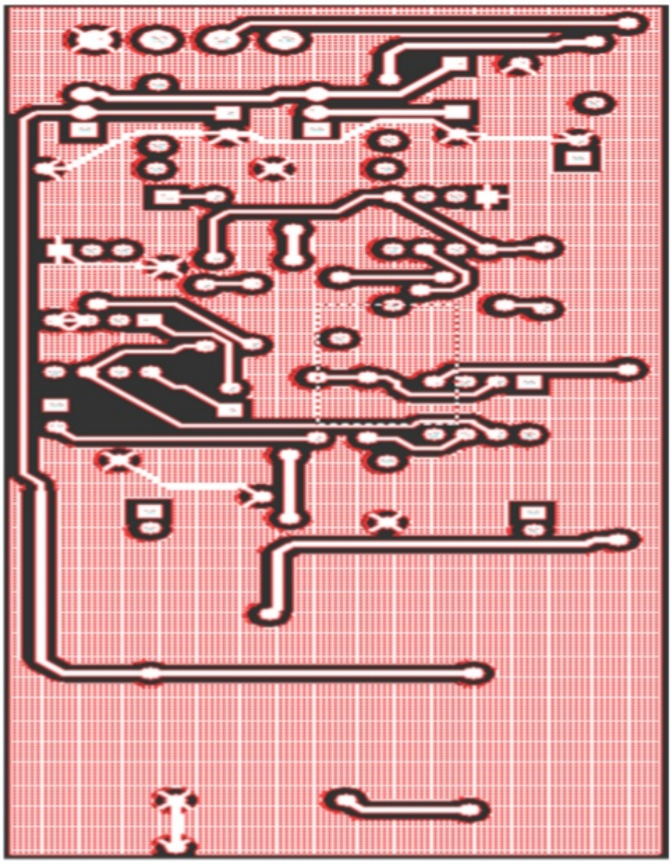


Figure 32: PCB bottom layer layout

38

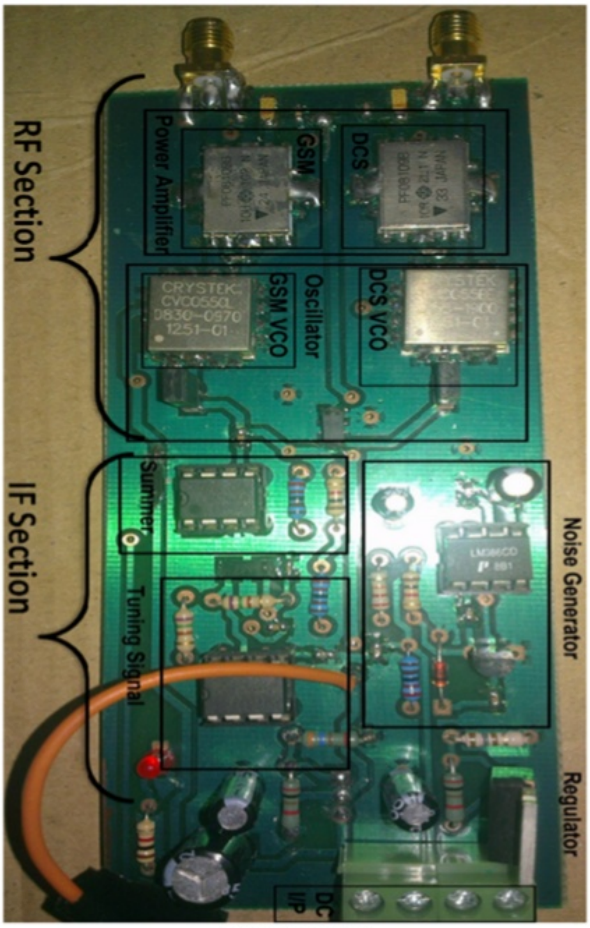


Figure 33: Jammer PCB

Jamming Test

a- **Obtained Spectrum Results:**

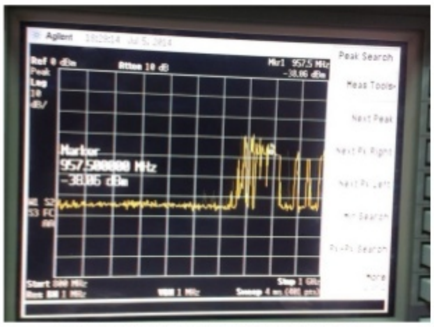


Figure 34: Output of the jammer's VCO at GSM 900

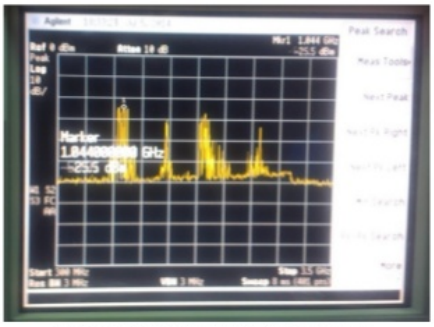


Figure 35: Output of the jammer's VCO at DCS 1800

Figure 34 and Figure 35 show the results of the spectrum analyzer taken from the VCOs in GSM and DCS frequency ranges. The results were taken from the VCOs as the spectrum analyzer we used has a limit to the input power up to 30 dBm. The resulting peak power is due to the attenuation in the device which reaches 10 dB. So, the results differ from the designed one.

b- Practical Jamming Test:

Table 8: Jammer effect's on Mobinil network's signal

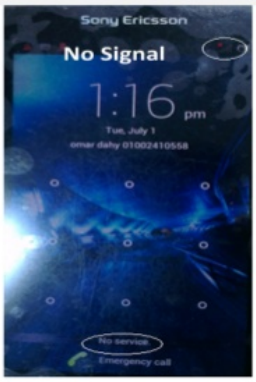
Mobinil	
Jammer OFF	**Jammer ON**
	

Table 9: Jammer effect's on Vodafone network's signal

Vodafone	
Jammer OFF	**Jammer ON**
	

The tables (8) and (9) show the status of the mobile. It can be clearly seen that the signal is "ON" when the jammer is "OFF", while the signal disappears when the jammer is "ON". This test was applied on the two operators Mobinil and Vodafone.

41

Chapter Six

6 CONCLUSION & FUTURE WORK

Presented By:-

1- Abdallah Mahmoud

2- Joumana Mohamed

3- Mohamed Atef

4- Suzy Sayed

In this project, which turned out to be a full success, we designed a device that stops phone ringing. This device could be used in places where ringing is not desired at specific times, as these ringings may disturb people in such places. The designed device works in dual band. It jams both the GSM 900 and GSM 1800 bands. The device was able to jam the two main cell phone carriers in Egypt.

We, as a team, learned more about the mobile phone's structure as the jammer components are similar to its architecture. We also knew more about the different frequency bands used in the mobile communication (GSM 900 – DCS 1800).

The project was implemented according to the following plan:

- We started by realizing how mobile jammer works and legal issues concerning using it.
- We studied jamming techniques to choose the best type that could match our aim. We illustrated each stage using block diagrams to clarify the concept concerning each section.
- We searched for components that are needed for building this device, and specified the main components which were :

- For the IF section, we used 555timer, Zener diode, mixer, PC power supply and some discrete components (resistors and capacitors).
- For RF section, we needed two VCO's that operate at the needed bands, two power amplifier, and two antennas.

- The schematic was drawn using OrCAD design software and PCB was built using OrCAD Layout.
- Design test was performed either by using simulation or using experiments as libraries of most of the components were not available
  - Some IF section simulations were performed and some were tested.
  - RF section components were not simulated but selected based on the datasheet and performance of each component.
- All the IF-components were bought from local companies. Then, the IF-section was built and tested.
- Some RF-components (VCO) were bought from Mouser Company. Others were taken from old used mobile phones.
- Finally we assembled and tested the jammer. Fortunately, we got positive results. Both bands were fully jammed.

Future Work:

- Smart jamming: jammer could be done using microcontrollers and computers.
- Jamming using frequency synthesizer: it jams the signal only at specific frequency by tuning the synthesizer and calculating some equations.

REFERENCES

[1] http://electronics.howstuffworks.com/cell-phone-jammer.htm

[2] *RABC M&PC Committee*, "Use of Jammer and Disabler Devices for Blocking PCS, Cellular and Related Services", [online].
Available: http://www.rabc.ottawa.on.ca/

[3] RICHARD A.POISEL, "Modern Communications Jamming Principles and Techniques", ARTECH House, 2004.

[4] S. Shah, S. Zafar, and S. Jafri, "GSM Jammer", 2006.

[5] A. Sedra, K. Smith, "MICROELECTRONIC CIRCUITS", OXFORD UNIVERSITY PRESS, 2004

[6] http://www.learningaboutelectronics.com

[7] http://www.circuitstoday.com/diode-clamping-circuits

[8] K. Siwiak, Radio-wave propagation and Antennas for personal communication.

[9] D. Pozar, "Microwave Engineering, John Wiley and Sons", 2005.

APPENDIX

PF08109B

MOS FET Power Amplifier Module
for E-GSM and DCS1800 Dual Band Handy Phone

RENESAS

ADE-208-821C (Z)

Rev.3
Feb. 2001

Application

- Dual band Amplifier for E-GSM (880 MHz to 915 MHz) and DCS1800 (1710 MHz to 1785 MHz)
- For 3.5 V nominal battery use

Features

- 2 in / 2 out dual band amplifire
- Simple external circuit including output matching circuit
- High gain 3stage amplifier : 0 dBm input Typ
- Lead less thin & Small package : 11 × 13.75 × 1.8 mm Typ
- High efficiency : 50% Typ at nominal output power for E-GSM
  43% Typ at 32.7 dBm for DCS1800

Pin Arrangement

• RF-O-12

1: N/C
2: N/C
3: Pout $_{DCS}$
4: Vdd $_{DCS}$
5: Vdd $_{GSM}$
6: Pout $_{GSM}$
7: N/C
8: Vtxlo
9: Pin $_{GSM}$
10: Vapc $_{GSM}$
11: Vapc $_{DCS}$
12: Pin $_{DCS}$
G: GND

46

PF08109B

Absolute Maximum Ratings

(Tc = 25°C)

Item	Symbol	Rating	Unit
Supply voltage	Vdd	8	V
Supply current	Idd_{GSM}	3	A
	Idd_{DCS}	2	A
Vtxlo voltage	Vtxlo	4	V
Vapc voltage	Vapc	4	V
Input power	Pin	10	dBm
Operating case temperature	Tc (op)	–30 to +100	°C
Storage temperature	Tstg	–30 to +100	°C
Output power	Pout GSM	5	W
	Pout DCS	3	W

Note: The maximum ratings shall be valid over both the E-GSM-band (880 MHz to 915 MHz), and the DCS1800-band (1710 MHz to 1785 MHz).

Electrical Characteristics for DC

(Tc = 25°C)

Item	Symbol	Min	Typ	Max	Unit	Test Condition
Drain cutoff current	Ids	—	—	100	µA	Vdd = 8 V, Vapc = 0 V
Vapc control current	Iapc	—	—	3	mA	Vapc =2.2 V
Vtxlo control current	Itxlo	—	—	100	µA	Vtxlo = 2.4 V

Electrical Characteristics for E-GSM mode

(Tc = 25°C)

Test conditions unless otherwise noted:
f = 880 to 915 MHz, Vdd $_{GSM}$ = 3.5 V, Pin $_{GSM}$ = 0 dBm, Rg = Rl = 50 Ω, Tc = 25°C, Vapc $_{DCS}$ = 0.1 V
Pulse operation with pulse width 577 μs and duty cycle 1:8 shall be used.

Item	Symbol	Min	Typ	Max	Unit	Test Condition
Frequency range	f	880	—	915	MHz	
Total efficiency (Hi)	$\eta_{T(H)}$	41	50	—	%	Pout $_{GSM}$ = 35.5dBm, Vtxlo = 0.1V, Vapc $_{GSM}$ = controlled
2nd harmonic distortion	2nd H.D.	—	–45	–38	dBc	
3rd harmonic distortion	3rd H.D.	—	–45	–40	dBc	
Input VSWR	VSWR (in)	—	1.5	3	—	
Total efficiency (Lo)	$\eta_{T(L)}$	27	35	—	%	Pout $_{GSM}$ = 30.8dBm, Vtxlo = 2.4V, Vapc $_{GSM}$ = controlled
Output power (1)(Hi)	Pout (1)(Hi)	35.5	36.0	—	dBm	Vapc $_{GSM}$ = 2.2V, Vtxlo = 0.1V
Output power (1)(Lo)	Pout (1)(Lo)	30.8	31.3	—	dBm	Vapc $_{GSM}$ = 2.2V, Vtxlo = 2.4V
Output power (2)(Hi)	Pout (2)(Hi)	33.5	34.0	—	dBm	Vdd $_{GSM}$ = 3.0V, Vapc $_{GSM}$ = 2.2V, Tc = +85°C, Vtxlo = 0.1V
Output power (2)(Lo)	Pout (2)(Lo)	28.8	29.3	—	dBm	Vdd $_{GSM}$ = 3.0V, Vapc $_{GSM}$ = 2.2V, Tc = +85°C, Vtxlo = 2.4V
Isolation	—	—	–42	–36	dBm	Vapc $_{GSM}$ = 0.2V, Vtxlo = 0.1V
Isolation at DCS RF-output when GSM is active	—	—	–23	–17	dBm	Pout $_{GSM}$ = 35.5dBm, Vtxlo = 0.1V Measured at f = 1760 to 1830MHz
Switching time	t_r, t_f	—	1	2	μs	Pout $_{GSM}$ = 0 to 35.5dBm, Vtxlo = 0.1V
Stability	—	No parasitic oscillation			—	Vdd $_{GSM}$ = 3.0 to 5.1V, Pout $_{GSM}$ ≤ 35.5dBm, Vtxlo = 0.1, 2.4V, Vapc $_{GSM}$ ≤ 2.2V, GSMpulse. Rg = 50Ω, Output VSWR = 6 : 1 All phases
Load VSWR tolerance	—	No degradation			—	Vdd $_{GSM}$ = 3.0 to 5.1V, t = 20sec., Pout $_{GSM}$ ≤ 35.5dBm, Vtxlo = 0.1, 2.4V, Vapc $_{GSM}$ ≤ 2.2V, GSM pulse. Rg = 50Ω, Output VSWR = 10 : 1 All phases

PF08109B

Electrical Characteristics for DCS1800 mode

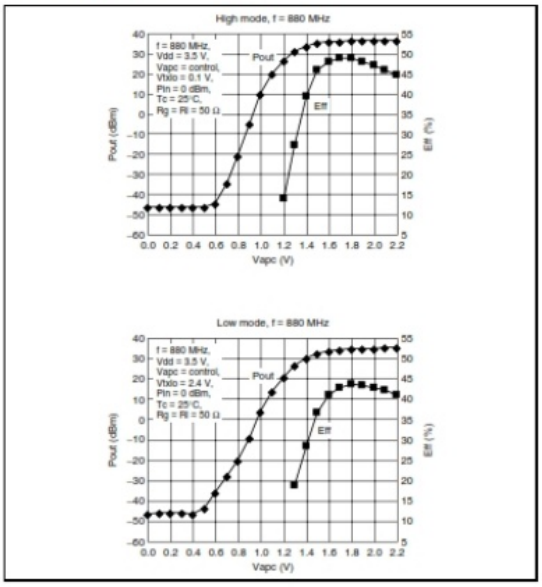
(Tc = 25°C)

Test conditions unless otherwise noted:
f = 1710 to 1785 MHz, Vdd_{DCS} = 3.5 V, Pin_{DCS} = 0 dBm, Rg = Rl = 50 Ω, Tc = 25°C, $Vapc_{GSM}$ =0.1 V
Pulse operation with pulse width 577 μs and duty cycle 1:8 shall be used.

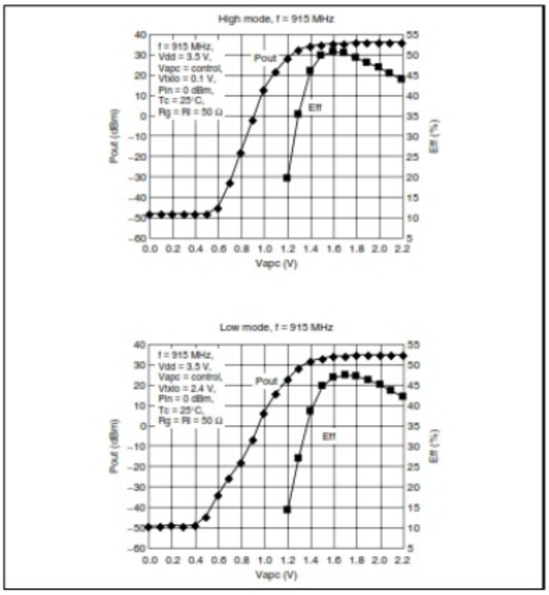
Item	Symbol	Min	Typ	Max	Unit	Test Condition
Frequency range	f	1710	—	1785	MHz	
Total efficiency (Hi)	η_{TDC}	36	43	—	%	$Pout_{DCS}$ = 32.7dBm, $Vapc_{DCS}$ = controlled
2nd harmonic distortion	2nd H.D.	—	−45	−38	dBc	
3rd harmonic distortion	3rd H.D.	—	−45	−40	dBc	
Input VSWR	VSWR (in)	—	1.5	3	—	
Total efficiency (Lo)	η_{TDC}	17	25	—	%	$Pout_{DCS}$ = 26.7dBm, $Vapc_{DCS}$ = controlled
Output power (1)	Pout (1)	32.7	33.2	—	dBm	$Vapc_{DCS}$ = 2.2V,
Output power (2)	Pout (2)	30.7	31.2	—	dBm	Vdd_{DCS} = 3.0V, $Vapc_{DCS}$ = 2.2V, Tc = +85°C
Isolation	—	—	−42	−36	dBm	$Vapc_{DCS}$ = 0.2V
Isolation at GSM RF-output when DCS is active	—	—	−10	0	dBm	$Pout_{DCS}$ = 32.7dBm, Measured at f = 1710 to 1785MHz
Switching time	t_r, t_f	—	1	2	μs	$Pout_{DCS}$ = 0 to 32.7dBm
Stability	—	No parasitic oscillation			—	Vdd_{DCS} = 3.0 to 5.1V, $Pout_{DCS}$ ≤ 32.7dBm, $Vapc_{DCS}$ ≤ 2.2V, DCS pulse. Rg = 50Ω, Output VSWR = 6 : 1 All phases
Load VSWR tolerance	—	No degradation			—	Vdd_{DCS} = 3.0 to 5.1V, $Pout_{DCS}$ ≤ 32.7dBm, t = 20sec., $Vapc_{DCS}$ ≤ 2.2V, DCS pulse. Rg = 50Ω, Output VSWR = 10 : 1 All phases

49

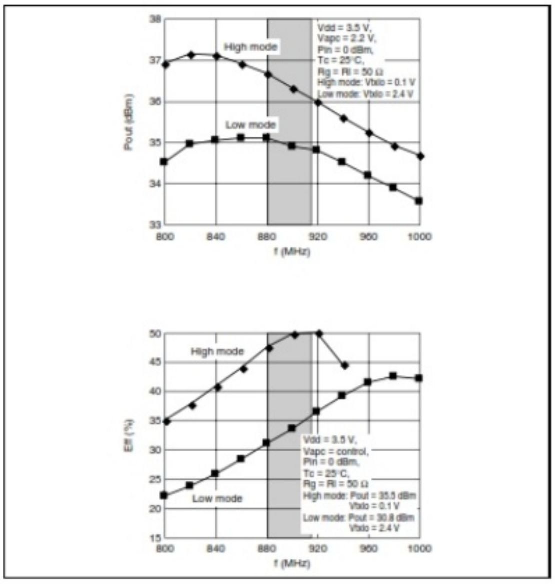
Characteristic Curves



PF08109B

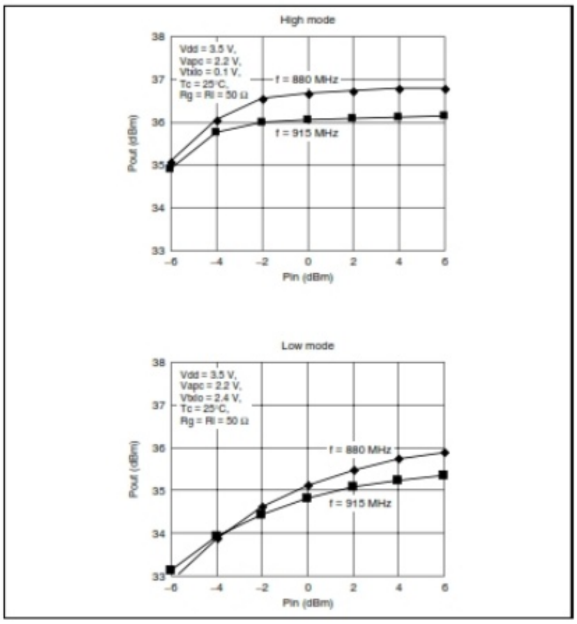

High mode, f = 915 MHz
f = 915 MHz,
Vdd = 3.5 V,
Vapc = control,
Vtxlo = 0.1 V,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
Pout
Eff
Pout (dBm)
Eff (%)
Vapc (V)
Low mode, f = 915 MHz
f = 915 MHz,
Vdd = 3.5 V,
Vapc = control,
Vtxlo = 2.4 V,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
Pout
Eff
Pout (dBm)
Eff (%)
Vapc (V)

PF08109B

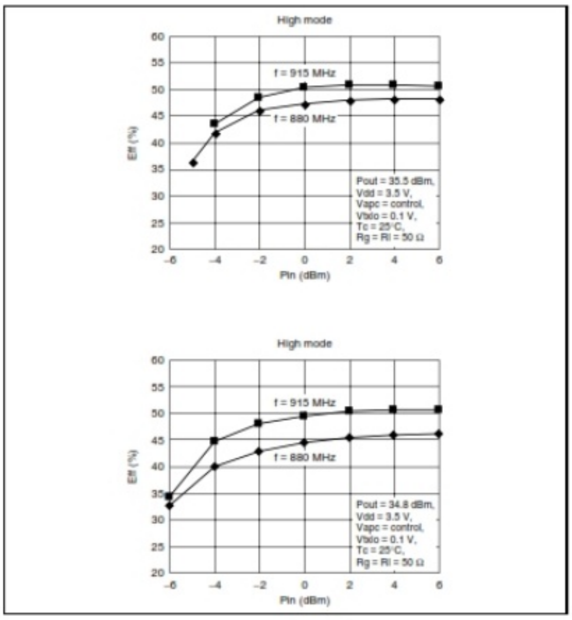

Vdd = 3.5 V,
Vapc = 2.2 V,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
High mode: Vbxlo = 0.1 V
Low mode: Vbxlo = 2.4 V
High mode
Low mode
Pout (dBm)
f (MHz)
Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
High mode: Pout = 35.5 dBm
Vbxlo = 0.1 V
Low mode: Pout = 30.8 dBm
Vbxlo = 2.4 V
High mode
Low mode
Eff (%)
f (MHz)

52

PF08109B

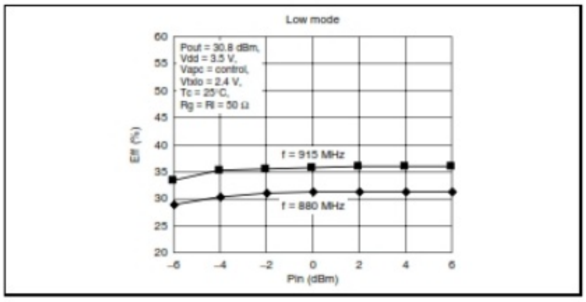

High mode
Vdd = 3.5 V,
Vapc = 2.2 V,
Vtxlo = 0.1 V,
Tc = 25°C,
Rg = Rl = 50 Ω
f = 880 MHz
f = 915 MHz
Pout (dBm)
Pin (dBm)
Low mode
Vdd = 3.5 V,
Vapc = 2.2 V,
Vtxlo = 2.4 V,
Tc = 25°C,
Rg = Rl = 50 Ω
f = 880 MHz
f = 915 MHz
Pout (dBm)
Pin (dBm)

PF08109B

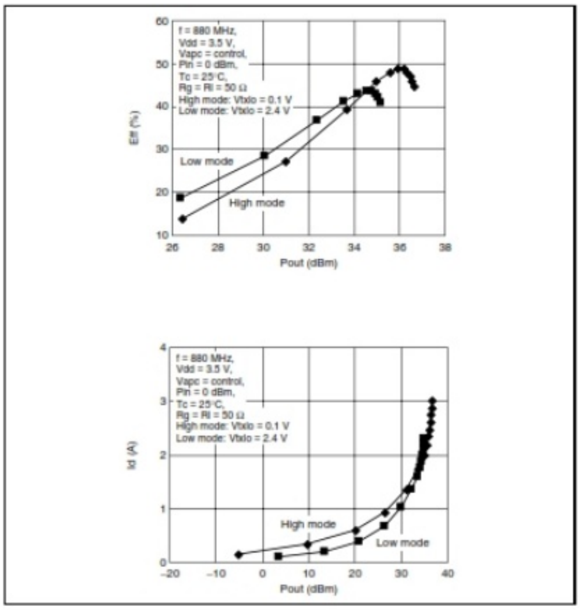

High mode
f = 915 MHz
f = 880 MHz
Eff (%)
Pin (dBm)
Pout = 35.5 dBm, Vdd = 3.5 V, Vapc = control, Vbio = 0.1 V, Tc = 25°C, Rg = Rl = 50 Ω
High mode
f = 915 MHz
f = 880 MHz
Eff (%)
Pin (dBm)
Pout = 34.8 dBm, Vdd = 3.5 V, Vapc = control, Vbio = 0.1 V, Tc = 25°C, Rg = Rl = 50 Ω

54

PF08109B

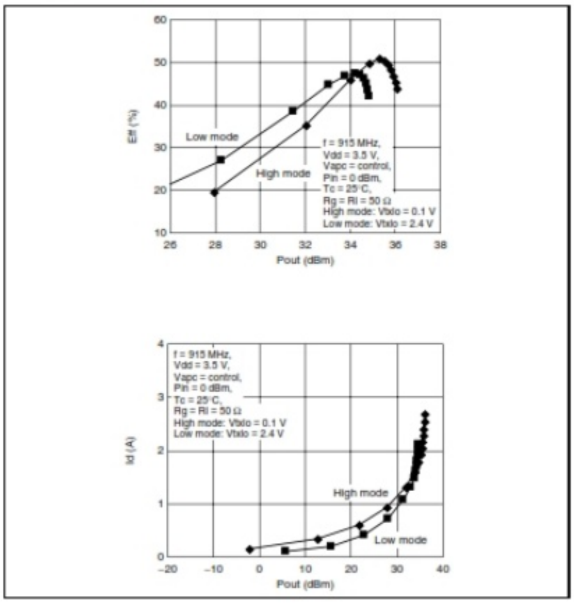

Low mode
Pout = 30.8 dBm,
Vdd = 3.5 V,
Vapc = control,
Vtxlo = 2.4 V,
Tc = 25°C,
Rg = Rl = 50 Ω
f = 915 MHz
f = 880 MHz
Eff (%)
Pin (dBm)
60
55
50
45
40
35
30
25
20
–6
–4
–2
0
2
4
6

PF08109B


f = 880 MHz,
Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
High mode: Vtxlo = 0.1 V
Low mode: Vtxlo = 2.4 V
Low mode
High mode
Eff (%)
Pout (dBm)
60
50
40
30
20
10
26
28
30
32
34
36
38
f = 880 MHz,
Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
High mode: Vtxlo = 0.1 V
Low mode: Vtxlo = 2.4 V
High mode
Low mode
Id (A)
Pout (dBm)
4
3
2
1
0
−20
−10
0
10
20
30
40

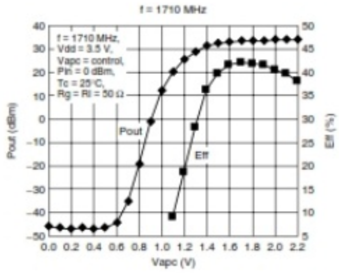
56

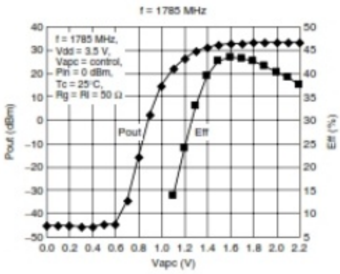
PF08109B


Eff (%)
Low mode
High mode
f = 915 MHz,
Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
High mode: Vtxlo = 0.1 V
Low mode: Vtxlo = 2.4 V
Pout (dBm)
Id (A)
f = 915 MHz,
Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
High mode: Vtxlo = 0.1 V
Low mode: Vtxlo = 2.4 V
High mode
Low mode
Pout (dBm)

57

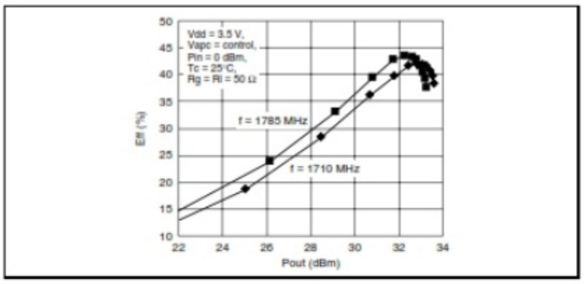
PF08109B


f = 1710 MHz
f = 1710 MHz,
Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
Pout
Eff
Pout (dBm)
Eff (%)
Vapc (V)


f = 1785 MHz
f = 1785 MHz,
Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
Pout
Eff
Pout (dBm)
Eff (%)
Vapc (V)

58

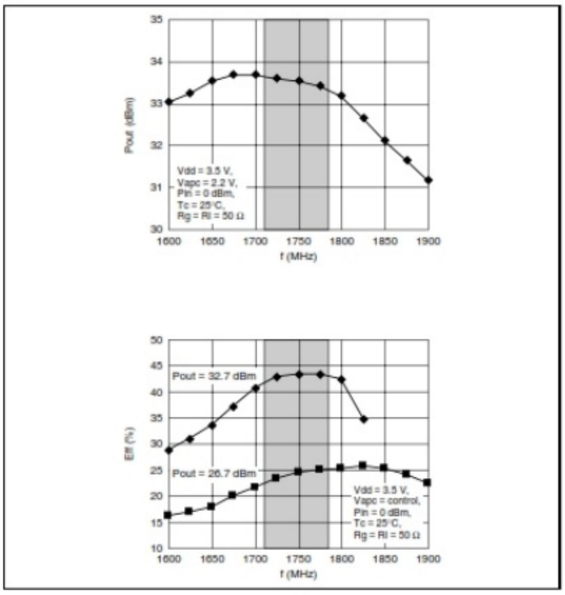
PF08109B



Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
f = 1785 MHz
f = 1710 MHz
Eff (%)
Pout (dBm)
50
45
40
35
30
25
20
15
10
22
24
26
28
30
32
34

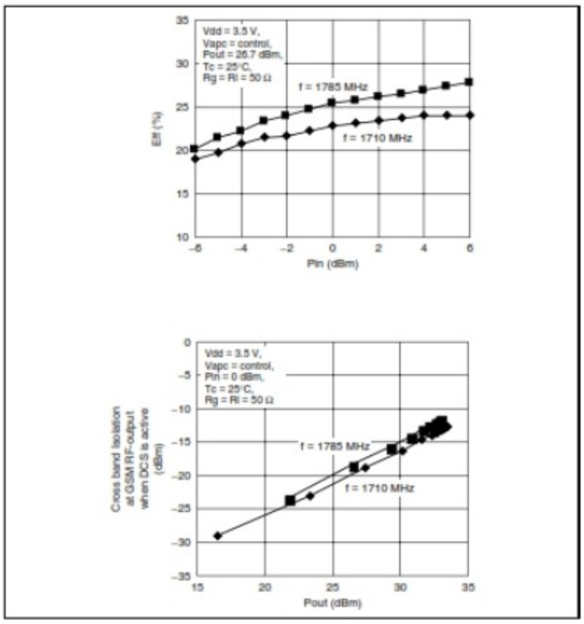
59

PF08109B

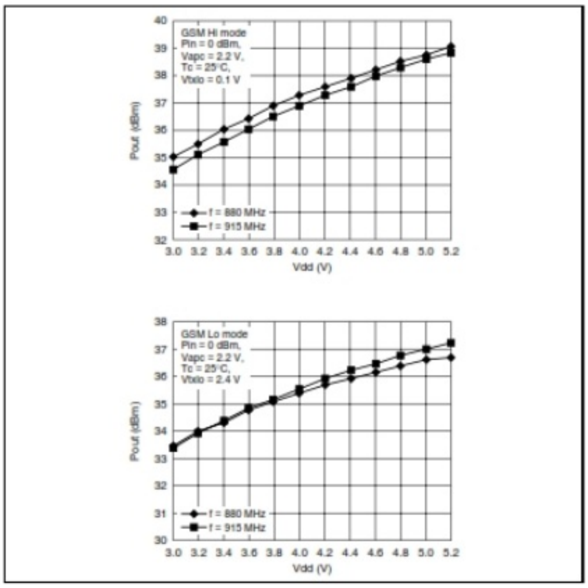


60

۶۱

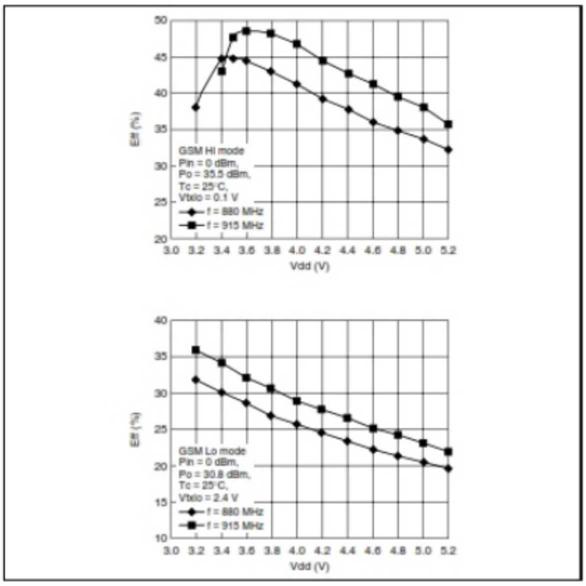

Vdd = 3.5 V,
Vapc = control,
Pout = 26.7 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
f = 1785 MHz
f = 1710 MHz
Eff (%)
Pin (dBm)
Vdd = 3.5 V,
Vapc = control,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
f = 1785 MHz
f = 1710 MHz
Cross band isolation at GSM RF-output when DCS is active (dBm)
Pout (dBm)

PF08109B


GSM Hi mode
Pin = 0 dBm,
Vapc = 2.2 V,
Tc = 25°C,
Vtxlo = 0.1 V
f = 880 MHz
f = 915 MHz
Pout (dBm)
Vdd (V)
GSM Lo mode
Pin = 0 dBm,
Vapc = 2.2 V,
Tc = 25°C,
Vtxlo = 2.4 V
f = 880 MHz
f = 915 MHz
Pout (dBm)
Vdd (V)

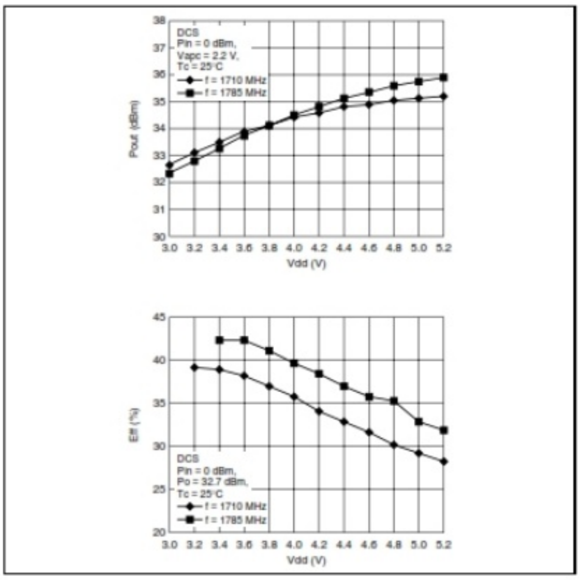
63

PF08109B

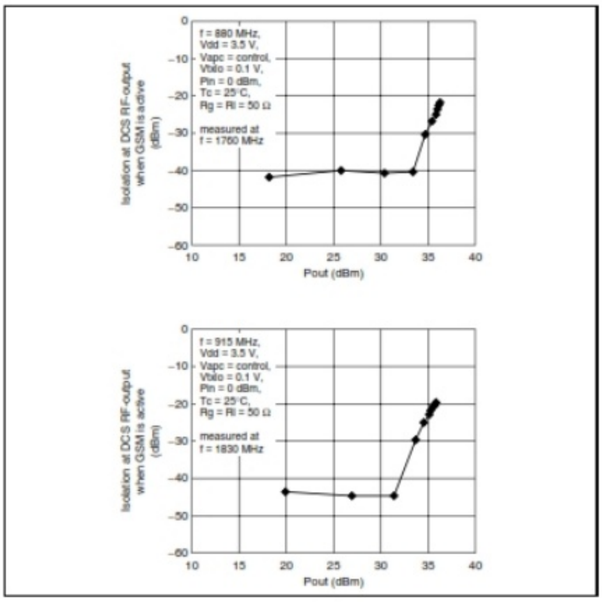

GSM Hi mode
Pin = 0 dBm,
Po = 35.5 dBm,
Tc = 25°C,
Vtxlo = 0.1 V
f = 880 MHz
f = 915 MHz
Eff (%)
Vdd (V)
GSM Lo mode
Pin = 0 dBm,
Po = 30.8 dBm,
Tc = 25°C,
Vtxlo = 2.4 V
f = 880 MHz
f = 915 MHz
Eff (%)
Vdd (V)

64

PF08109B

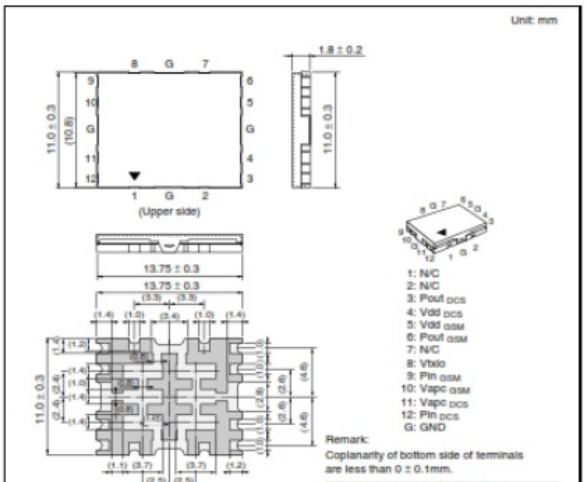

DCS
Pin = 0 dBm,
Vapc = 2.2 V,
Tc = 25°C
f = 1710 MHz
f = 1785 MHz
Pout (dBm)
Vdd (V)
DCS
Pin = 0 dBm,
Po = 32.7 dBm,
Tc = 25°C
f = 1710 MHz
f = 1785 MHz
Eff (%)
Vdd (V)

PF08109B


f = 880 MHz,
Vdd = 3.5 V,
Vapc = control,
Vbllo = 0.1 V,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
measured at
f = 1760 MHz
Isolation at DCS RF-output when GSM is active (dBm)
Pout (dBm)
0
−10
−20
−30
−40
−50
−60
10
15
20
25
30
35
40
f = 915 MHz,
Vdd = 3.5 V,
Vapc = control,
Vbllo = 0.1 V,
Pin = 0 dBm,
Tc = 25°C,
Rg = Rl = 50 Ω
measured at
f = 1830 MHz
Isolation at DCS RF-output when GSM is active (dBm)
Pout (dBm)

PF08109B

Package Dimensions



Hitachi Code	RF-O-12
JEDEC	—
JEITA	—
Mass (reference value)	—

CRYSTEK MICROWAVE
A DIVISION OF CRYSTEK CORPORATION

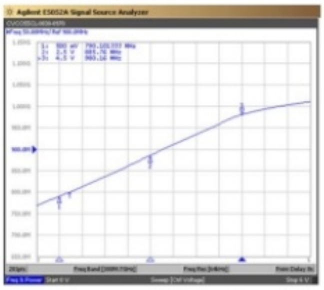
Voltage Controlled Oscillator-VCO
CVCO55CL-0830-0970

PERFORMANCE SPECIFICATION	MIN	TYP	MAX	UNITS
Lower Frequency:			830	MHz
Upper Frequency:	970			MHz
Tuning Voltage:	0.5		4.5	VDC
Supply Voltage:	4.75	5.0	5.25	VDC
Output Power:	+1.0	+4.0	+7.0	dBm
Supply Current:			30	mA
Harmonic Suppression (2nd Harmonic):		-15		dBc
Pushing:		1.0	2.0	MHz/V
Pulling, all Phases:		1.0	2.0	MHz pk-pk
Tuning Sensitivity:		52		MHz/V
Phase Noise @ 10kHz offset:		-106		dBc/Hz
Phase Noise @ 100kHz offset:		-126		dBc/Hz
Load Impedance:		50		Ω
Input Capacitance:			200	pF
Operating Temperature Range:	-40		+85	°C
Storage Temperature Range:	-45		+90	°C

RoHS Compliant

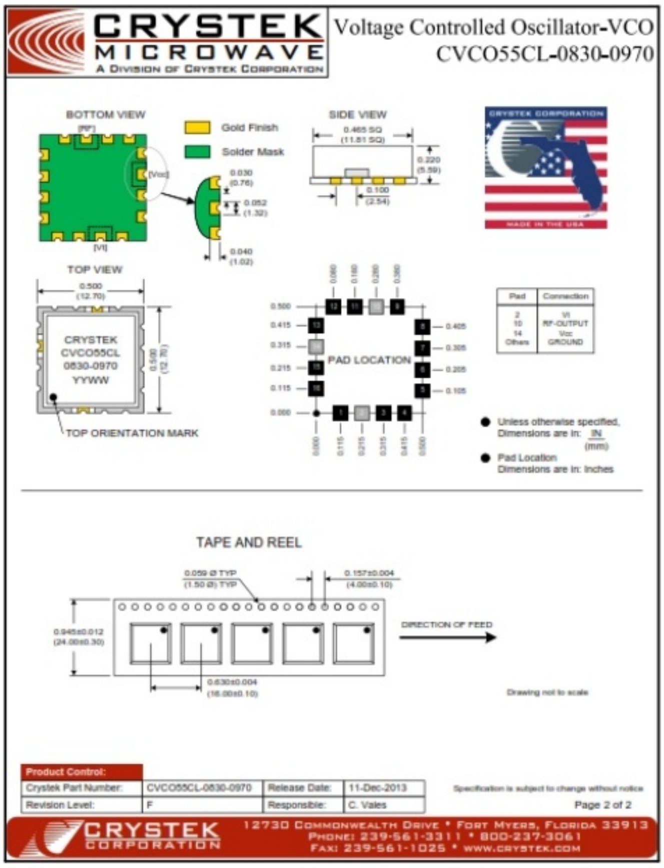
Phase Noise (1 Hz BW, Typical)

Tuning Curve (Typical)



Page 1 of 2

CRYSTEK CORPORATION
12730 Commonwealth Drive • Fort Myers, Florida 33913
Phone: 239-561-3311 • 800-237-3061
Fax: 239-561-1025 • www.crystek.com



CRYSTEK MICROWAVE
A Division of Crystek Corporation

Voltage Controlled Oscillator-VCO
CVCO55CL-0830-0970

BOTTOM VIEW
[RF]
[Vcc]
[Vt]
Gold Finish
Solder Mask
0.030 (0.76)
0.052 (1.32)
0.040 (1.02)

SIDE VIEW
0.465 SQ (11.81 SQ)
0.220 (5.59)
0.100 (2.54)

CRYSTEK CORPORATION
MADE IN THE USA

TOP VIEW
0.500 (12.70)
CRYSTEK
CVCO55CL
0830-0970
YYWW
0.500 (12.70)
TOP ORIENTATION MARK

PAD LOCATION

Pad	Connection
2	Vt
10	RF-OUTPUT
14	Vcc
Others	GROUND

- Unless otherwise specified, Dimensions are in: IN (mm)
- Pad Location Dimensions are in: Inches

TAPE AND REEL

0.059 Ø TYP (1.50 Ø) TYP
0.157±0.004 (4.00±0.10)
0.945±0.012 (24.00±0.30)
DIRECTION OF FEED
0.630±0.004 (16.00±0.10)
Drawing not to scale

Product Control:			
Crystek Part Number:	CVCO55CL-0830-0970	Release Date:	11-Dec-2013
Revision Level:	F	Responsible:	C. Vales

Specification is subject to change without notice

Page 2 of 2

CRYSTEK CORPORATION
12730 Commonwealth Drive • Fort Myers, Florida 33913
Phone: 239-561-3311 • 800-237-3061
Fax: 239-561-1025 • www.crystek.com

70

CRYSTEK MICROWAVE
A DIVISION OF CRYSTEK CORPORATION

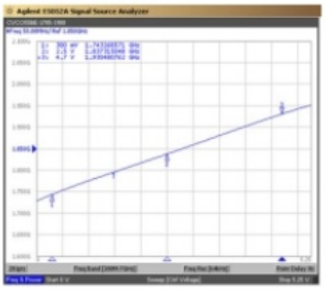
Voltage Controlled Oscillator-VCO
CVCO55BE-1785-1900

PERFORMANCE SPECIFICATION	MIN	TYP	MAX	UNITS
Lower Frequency:			1785	MHz
Upper Frequency:	1900			MHz
Tuning Voltage:	0.3		4.7	VDC
Supply Voltage:	4.75	5.0	5.25	VDC
Output Power:	0	+2.5	+5.0	dBm
Supply Current:			35	mA
Harmonic Suppression (2nd Harmonic):		-15		dBc
Pushing:			2.0	MHz/V
Pulling, all Phases:			3.0	MHz pk-pk
Tuning Sensitivity:		45		MHz/V
Phase Noise @ 10kHz offset:		-100		dBc/Hz
Phase Noise @ 100kHz offset:		-122		dBc/Hz
Load Impedance:		50		Ω
Input Capacitance:			50	pF
Operating Temperature Range:	-40		+85	°C
Storage Temperature Range:	-45		+90	°C

RoHS Compliant

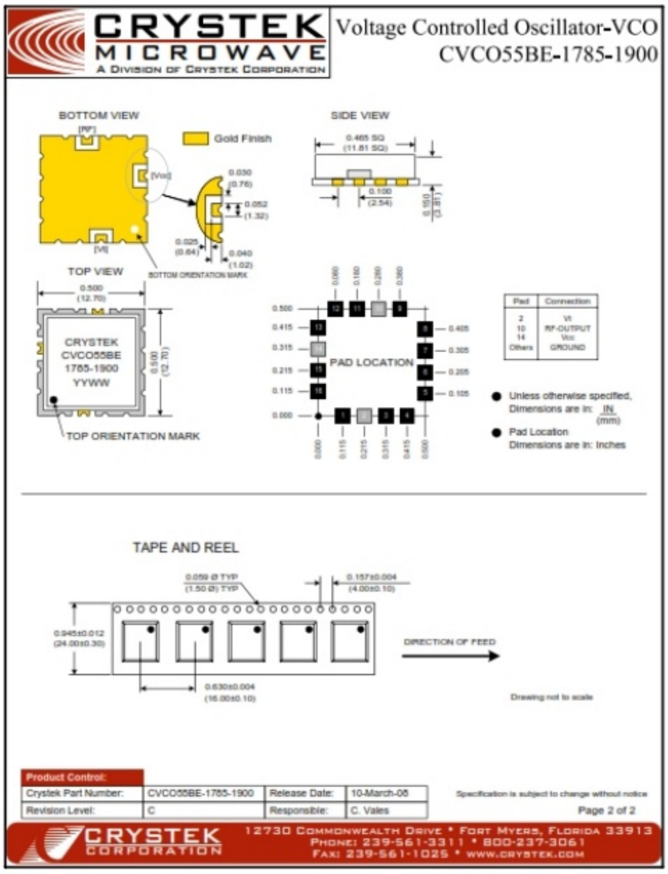
Phase Noise (1 Hz BW, Typical)

Tuning Curve (Typical)



Page 1 of 2

CRYSTEK CORPORATION
12730 COMMONWEALTH DRIVE • FORT MYERS, FLORIDA 33913
PHONE: 239-561-3311 • 800-237-3061
FAX: 239-561-1025 • WWW.CRYSTEK.COM



72

Upcoming SlideShare

Loading in …۵

×

۶۰ of ۸۰

Dual-Band Mobile Phone Jammer

Mohamed Atef, Electronics & Communications Engineering Student

Follow

Published on Sep ١٢, ٢٠١۴

Our graduation project talks about how to prevent mobile phones from receiving

...

Published in: Engineering

- ۰ Comments
- ۸ Likes
- Statistics
- Notes

- Full Name
  Comment goes here.
  ۱۲ hours ago Delete Reply Spam Block
  Are you sure you want to Yes No
  Your message goes here

Share your thoughts…
Post

- *Be the first to comment*

- jinluo۱۳۶۸
  ۳ months ago
- ronggonabdullah
  ۴ months ago
- 
  Vamshi Pragnapuram , Volunteer at The Art of Living
  ۴ months ago
- FrankMulla۸۷
  ۷ months ago
- Sridhar Sahu
  ۷ months ago

Show More
No Downloads
Views
Total views
۳,۰۷۴
On SlideShare
۰
From Embeds
۰
Number of Embeds
۳۲
Actions
Shares
۵
Downloads
۳۴۶
Comments
۰
Likes
۸

Embeds •

No embeds

No notes for slide

Dual-Band Mobile Phone Jammer

1. ۱. Arab Academy for Science, Technology and Maritime Transport College of Engineering and Technology Electronics and Communications B. Sc. Final Year Project Dual-Band Mobile Jammer Presented By: Abdallah Mahmoud ۹۱۰۴۰۸۵ Joumana Mohamed ۹۱۰۳۴۰۵ Mohamed Atef ۹۱۰۴۶۵۷ Suzy Sayed ۹۱۰۴۲۵۰ Supervised By: Prof. Dr. Hesham El Badawy J u l y ۲ ۰ ۱ ۴
2. ۲. ii DECLARATION We hereby certify that this material, which we now submit for assessment on the programme of study leading to the award of Bachelor of Science in Electronics and Communication Engineering is entirely our own work, that we have exercised reasonable care to ensure that the work is original, and does not to the best of our knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of our work. Signed: ۱-Abdallah Mahmoud ۲-Joumana Mohamed ۳-Mohamed Atef ۴-Suzy Sayed Registration No.: ۱-۹۱۰۴۰۸۵ ۲-۹۱۰۳۴۰۵ ۳-۹۱۰۴۶۵۷ ۴-۹۱۰۴۲۵۰ Date: ۷th July ۷, ۲۰۱۴
3. ۳. iii ACKNOWLEDGMENT First of all, we would like to thank everyone helped us along this journey from the very beginning till we achieved our final product. Special thanks to Prof. Hesham Elbadawy for his ultimate assistance, whose guidance, advice, and supervision was invaluable. We also deeply thank Eng. Nagdy from the NTI for his generous help and support. Finally, we would like to thank the Arab Academy for Science and Technology and Maritime Transport. Their hospitality and support during the period this project took place are greatly acknowledged.
4. ۴. iv ABSTRACT Nowadays, mobile communication has become so spread. In order that, a lot of places, organizations, or facilities require to keep quiet, on other words, some of these organizations may preserve some sort of security, so, mobile jammer has become an essential device to be used for such applications to minimize the mobile access inside different organizations or firms. The project presents a general outline of mobile jammer instrument, giving short note about its civilian and military usage. In addition it provides insight into how the mobile jammer works. It describes the jamming techniques and gives brief explanation of the design parameters and specifications. The report presents the system implementation design by giving general information about each section that is used in the design. It explains all electronic components used in each section in the hardware part. Also, it shows the results that have been achieved in experiments in the form of hardware and software. Finally, the report mentions some future work related to the jammers technologies.
5. ۵. v TABLE OF CONTENTS
6. ۶. vi LIST OF FIGURES

۷. ۷.

۸. ۸. viii LIST OF ABBREVIATIONS Op-Amp Operational Amplifier IC Integrated Circuit PCB Printed Circuit Board DC Direct current AC Alternative Current GSM Global System for Mobile Communication DCS Digital Cellular System PCS Personal Communication Services RF Radio Frequency EMI shield Electromagnetic Shield BBN Broadband Noise BTS Base Station Transceiver SNR Signal to Noise Ratio IF Intermediate Frequency PC Personal Computer VCO Voltage Controlled Oscillator ADS Software Advanced Design System Software VSWR Voltage Standing Wave Ratio FR-۴ Flame Retardant-۴ AJ Anti Jamming

۹. ۹. ۱ C h a p t e r O n e ۱ INTRODUCTION Presented By:- ۱- Abdallah Mahmoud ۲- Joumana Mohamed ۳- Mohamed Atef ۴- Suzy Sayed Mobile (or cell) phones are becoming essential tools in our daily life. Needless to say, the wide use of mobile phones could create some problems as the sound of ringing becomes annoying. This could happen in some places like conference rooms, law courts, libraries, lecture rooms, masajed and in examination rooms in schools and colleges which can limit the cheating phenomenon happen there. From this point, the idea of mobile jammers appears. A mobile jammer is an instrument used to prevent cellular phones from receiving signals from base stations. When used, the jammer effectively disables cellular phones. These devices can be used in practically any location, but are found primarily in places where a phone call would be particularly disruptive because silence is expected. Mobile jammers were originally developed for law enforcement and military applications to interrupt communications by criminals and terrorists. [۱] Mobile phones are commonly designed to operate across several bands. In most circumstances, a jammer would also need to operate across the same bands to effectively jam mobile phones within range. The geographical range of a mobile phone jammer depends on its power level, its operating frequencies, the physical situation of the jammer, the mobile phone/s it is attempting to block, and the local environment. Our aim in this project is to design, implement, and test a dual band mobile jammer. This jammer works at different frequencies such as: GSM ۹۰۰ and DCS۱۸۰۰.

۱۰. ۱۰. ۲ C h a p t e r T w o ۲ CELL PHONE JAMMER Presented By:- ۱- Abdallah Mahmoud ۲- Joumana Mohamed ۳- Mohamed Atef ۴- Suzy Sayed ۲.۱ THEORY OF OPERATION As cell phones are full-duplex devices, which means they use two separate frequencies, one for talking and one for listening simultaneously. Some jammers block only one of the frequencies used by cell phones, which has the effect of blocking both. The phone is tricked into thinking there is no service because it can receive only one of the frequencies. As shown in figure۱, jamming devices overpower the cell phone by transmitting a signal on the same frequency and at a high enough power that the two signals collide and cancel each other out. Cell phones are designed to add power if they experience low-level interference, so the jammer must recognize and match the power increase from the phone.

۱۱. ۱۱. Figure ۱: Cell phone jammer To jam a cell phone, all you need is a device that broadcasts on the correct frequencies. Although different cellular systems process signals differently, all cell-phone networks use radio signals that can be interrupted. GSM, used in digital cellular and PCS-based ۳ systems, operates in the ۹۰۰-MHz and ۱۸۰۰-MHz bands in Europe and Asia. [۱] ۲.۲ CELL PHONE JAMMING LEGAL ISSUES In the United States, United Kingdom, Australia and many other countries, blocking cell-phone services (as well as any other electronic transmissions) is against the law. In fact, the "manufacture, importation, sale or offer for sale, including advertising, of devices designed to block or jam wireless transmissions is prohibited" as well. In most countries, it is illegal for private citizens to jam cell-phone transmission, but some countries are allowing businesses and government organizations to install jammers in areas where cell-phone use is seen as a public nuisance. In December ۲۰۰۴, France legalized cell-phone jammers in movie theaters, concert halls and other places with performances. France is finalizing technology that will let calls to emergency services go through. India has installed jammers in parliament and some prisons. It has been reported that universities in Italy have adopted the technology to prevent cheating. Students were taking photos of tests with their camera phones and sending them to classmates.[۱]

۱۲. ۱۲. ۴ Figure ۲: Mobile jammer in a meeting ۲.۳ JAMMING TECHNIQUES ۲.۳.۱ Type "A" Device (Jammers) This type of device comes equipped with several independent oscillators transmitting 'jamming signals' capable of blocking frequencies used by paging devices as well as those used by cellular/PCS systems' control channels for call establishment. When active in a designated area, such devices will (by means of RF interference) prevent all pagers and mobile phones located in that area from receiving and transmitting calls. ۲.۳.۲ Type "B" Device (Intelligent Cellular Disablers) Unlike jammers, Type "B" devices do not transmit an interfering signal on the control channels. The device, when located in a designated 'quiet' area, functions as a 'detector'. It has a unique identification number for communicating with the cellular base station. When a Type "B" device detects the presence of a mobile phone in the quiet room; the 'filtering' (i.e. the prevention of authorization of call establishment) is done by the software at the base station ۲.۳.۳ Type "C" Device (Intelligent Beacon Disablers) Unlike jammers, Type "C" devices do not transmit an interfering signal on the control channels. The device, when located in a designated 'quiet' area, functions as a 'beacon' and any compatible terminal is instructed to disable its ringer or disable its operation, while within the coverage area of the beacon. Only terminals which have a compatible

۱۳. ۱۳. receiver would respond and this would typically be built on a separate technology from cellular/PCS e.g., cordless wireless, paging, Bluetooth, …. On leaving the coverage area of the beacon, the handset must re-enable its normal function. ۲.۳.۴ Type "D" Device (Direct Receive & Transmit Jammers) This jammer behaves like a small, independent and portable base station, which can directly interact intelligently or unintelligently with the operation of the local mobile phone. The jammer is predominantly in receiving mode and will intelligently choose to interact and block the cell phone directly if it is within close proximity of the jammer. ۲.۳.۵ Type "E" Device (EMI Shield - Passive Jamming) This technique is using EMI suppression techniques to make a room into what is called a Faraday cage. Although labor intensive to construct, the Faraday cage essentially blocks, or greatly attenuates, virtually all electromagnetic radiation from entering or leaving the cage – or in this case a target room. [۲] Then we can conclude all these types with the below table indicating the status of each type as shown in table ۱ ۵ Table ۱: Comparison between different jamming techniques Type Emergency calls Efficiency Regularity Approval Implementation A Blocked Low Not allowed Very simple B Allowed Medium Required Complex (required third party)

C Allowed High Required Complex (required intelligent handset) D Allowed Medium Required Simple E Blocked High (no signal transmitted) Allowed Simple

۱۴. ۱۴. ۶ C h a p t e r T h r e e ۳ DESIGN PARAMETERS & SPECIFICATIONS Presented By:- ۱- Abdallah Mahmoud ۲- Joumana Mohamed ۳- Mohamed Atef ۴- Suzy Sayed ۳.۱ NOISE JAMMING For noise jamming, the jamming carrier signal is modulated with random noise waveform. The intent is to disrupt the AJ communication waveform by inserting the noise into the receiver. The bandwidth of the signal can be as wide as the entire spectrum width used by the AJ system or much narrower, occupying only a single channel Broadband Noise Jamming Broadband noise (BBN) jamming places noise energy across the entire width of the frequency spectrum used by the target radios. It is also called full band jamming and is sometimes called barrage jamming. This type of jamming is useful against all forms of AJ communications. This type of jamming essentially raises the background (thermal) noise level at the receiver, creating a higher noise environment for the AJ system. Noise is the nemesis for any communication system, and if the noise level can be increased it makes it more difficult for the communication system to operate. [۳]

۱۵. ۱۵. ۷ ۳.۲ FREQUENCY BAND The basic purpose of a GSM Mobile Jammer is to block or hinder communication between the Base Transceiver Station and the Mobile Station. This can only be achieved by rendering the transmission between them incomprehensible. The basic technique for accomplishing this goal is to create disturbance on the GSM transmission frequencies. In our project we want to jam on both GSM ۹۰۰ and GSM ۱۸۰۰ (DCS) so, we want to know the uplink and downlink frequencies for both of them and this was shown in table۲ Table ۲: Operating frequency band UPLINK (Handset transmit) DOWNLINK (Handset receive) USED IN EGYPT BY: GSM ۹۰۰ ۸۹۰-۹۱۵ MHz ۹۳۵-۹۶۰ MHz Vodafone- Mobinil DCS ۱۸۰۰ ۱۷۱۰-۱۷۸۵ MHz ۱۸۰۵-۱۸۸۰ MHz Vodafone- Mobinil- Etisalat Figure ۳: Mobile jammer effect on noise floor frequency Power spectral density The problem with jamming the entire band or the uplink frequencies is that we are aiming to disrupt communication at the BTS. For this we need a very high power transmitter that will create a powerful signal strong enough to reach the BTS. Furthermore, this action will cause the Signal to Noise ratio at the BTS to fall which will, in effect, cause all incoming signals at the BTS to be corrupted. Thus all incoming connections to the BTS

۱۶. ۱۶. will be disturbed which will jam the Mobile Stations throughout the entire coverage region of the BTS i.e. its cell. In contrast, if we create disturbance over the Downlink frequencies, we only need a transmitter powerful enough to create a signal that disrupts communication in our required area. This causes only the Mobile Stations in the specific area to be jammed and leaves the ones outside it alone. Summing it all up, we get the following result: Jamming the uplink or entire band requires a high power transmitter and disrupts ۸ communication over an entire cell Jamming the downlink band requires a transmitter of sufficient power to jam the required area only and does not disturb the communication outside it.[۴] Therefore, our goal is to disrupt communication over downlink frequencies only. ۳.۳ JAMMING ZONE This parameter is very important in our design, since the amount of the output power of the jammer depends on the area that we need to jam. Our design is established upon = ۱۰ for DCS ۱۸۰۰ band and = ۲۰ for GSM ۹۰۰ band. ۳.۴ FREE SPACE LOSS It is the loss in signal strength of an electromagnetic wave that would result from a line-of- sight path through free space. Free space path loss could be calculated through eq.۱ = ۳۲.۴۵ + ۲۰ + ۲۰ (dB) (۱) Where, The maximum free space loss (worst case F) happens when the maximum frequency is used in eq.۱. Using ۱۸۸۰ MHz and D=۱۰ meters gives: = ۳۲.۴۵ + ۲۰ (۰.۰۱) + ۲۰ (۱۸۸۰) =

۱۷. ۱۷. ۹ ۳.۵ JAMMING TO SIGNAL RATIO (J/S) Jamming is successful when the jamming signal denies the usability of the communication transmission. Usually, a successful jamming attack requires that the jammer power is roughly equal to signal power at the receiver (mobile device). The general equation of the jamming-to-signal ratio is given as follows in eq.۲ = (۲) Where: =Jammer Power = Antenna Gain from Jammer to Receiver =Antenna Gain from Receiver to Jammer =Range between Communication Transmitter and Receiver =Communication Receiver Bandwidth =Communication Signal Loss =Transmitter Power = Antenna Gain from Transmitter to Receiver =Antenna Gain from Receiver to Transmitter =Range between Jammer and Communication Receiver =Jammer Bandwidth =Jamming Signal Loss. So the SNR of the jammer in eq.۳ = (۳) Where S=mobile station signal power receiver and J= jammer power at mobile receiver. And the S = −۱۵dBm For GSM, the specified SNR = ۹ dB

۱۸. ۱۸. ۱۰ This will be used as the worst case scenario of the jammer in order to have maximum jamming power This could be clearly clarified in figure ۳: Figure ۴: Best and worst case of jamming This figure shows the best and the worst case according to jamming point of view. As we have a mobile near to the base station (worst case) we can conclude that this mobile received a high power from the base station so if we want to jam this one, we should have a high power of jamming to overflow its received power. In contrast, if we have a mobile further from the base station it will receive a power much lower than the previous case and this will be best case for jamming as it does not need high power to jam.

۱۹. ۱۹. ۱۱ ۳.۶ POWER CALCULATIONS Here in this part, we want to calculate the needed power in order to jam a cell phone within a distance of ۱۰ m for DCS and ۲۰ m for GSM ۹۰۰ , from the above considerations we shall calculate for the worst case (= ۹ , = −۱۵) in order to be sure we will have a jamming in everywhere as in eq.۴ ( ) >= − (۴) Therefore, >= −۲۴ Taking into account the free space loss as we calculate it before in eq.۱ and substitute in eq.۵ = + (۵) Therefore, = −۲۴ + ۵۸ = ۳۴ So, this power will be needed for the worst case for jamming the specified region.

۲۰. ۲۰. ۱۲ C h a p t e r F o u r ۴ SYSTEM IMPLEMENTATION Presented By:- ۱- Abdallah Mahmoud ۲- Joumana Mohamed ۳- Mohamed Atef ۴- Suzy Sayed Figure ۵: Jamming system block diagram ۴.۱ POWER SUPPLY It is used to supply both sections IF and RF with their suitable voltages. Any power supply consists of the following main parts: i. Transformer: - is used to transform the ۲۲۰VAC to other levels of voltages ii. Rectification: this part is to convert the AC voltage to a DC. We have two methods for rectifications:

۲۱. ۲۱. a. Half wave-rectification: the output voltage appears only during positive ۱۳ cycles of the input signal. b. Full wave -rectification: a rectified output voltage occurs during both the positive and negative cycles of the input signal. iii. The Filter: used to eliminate the fluctuations in the output of the full wave rectifier iv. Regulator: this is used to provide a desired DC-voltage Figure ۶: Power Supply block diagram Our aim is to get +۱۲, -۱۲, ۵, ۳.۵ and ۲.۴ volts in our design. We can get all values direct from PC power supply except ۲.۴ volt, this value we can get from regulator circuit. The regulator circuit consists of: ۱) LM۳۱۷ Regulator ۲) Two resistors ۳) Two capacitors Our equation of variable regulator as in eq.۶ = ۱.۲۵ ۱ + (۶)

۲۲. ۲۲. Where and are selected according to our required voltages. In our design of the regulator circuit we have first the LM۳۱۷ regulator which consists of: Input, output, and adjustment pins as shown in the below figure ۶: ۱۴ Figure ۷: LM۳۱۷ regulator Then, we connect this IC with two resistors to get the desired voltage, and connect two capacitors one at the input and the other at the output of the regulator used for the stability of the regulator's control loop [۶] as shown in the circuit of figure ۷: Figure ۸: Regulator circuit In order to calculate the ۲.۴ volt we have to select two resistors to give the required voltage. Put = ۱۶۰ Ω and = ۱۴۸ Ω and substitute in the above equation we will get = ۲.۴۰۶ , then take this voltage from the output pin.

۲۳. ۲۳. ۱۵ ۴.۲ INTERMEDIATE FREQUENCY (IF) SECTION An intermediate frequency (IF) is a frequency to which a carrier is shifted as an intermediate step in transmission or reception. The IF Section is the section which generates the tuning voltage for the VCO in the RF Section so that the output of the VCO is swept through the desired range of frequencies. The output of the IF Section is triangular wave of frequency ۱۰KHz to which noise is added and then the signal is offset by a certain DC value to obtain the required tuning voltage. Figure ۹: IF Section block diagram The components of the IF Section are as follows: Table ۳: IF Section components Triangular Wave Generator ۵۵۵ Timer IC Noise Generator Zener Diode Signal Mixer OpAmp in Summing configuration Offset Circuit Diode Clamper

۲۴. ۲۴. ۴.۲.۱ Triangular Wave Generator The main use of the triangular wave is to sweep the VCO through the desired frequency range. In the design, we shall use ۵۵۵timer IC operating in the astable mode to generate the sweeping signal. First, the output frequency and voltage depends on the charging and discharging of the capacitor and resistor values .The voltage depends on power supply for the IC as frequency is independent of the supply voltage. To determine the output sweeping voltage ۱۶ = ۲ ۳ = ۱ ۳ So the output voltage will swing between To determine the output frequency: The charge time ( ) is given by eq.۷ = ۰.۶۹۳ (+) ∗ (۷) The discharge time ( ) is given by eq.۸ = ۰.۶۹۳ ∗ ∗ (۸) By sub eq.۷ & eq.۸ to get the total period ( ) in eq.۹ = + = ۰.۶۹۳(+ ۲ ∗) ∗ (۹) The frequency of oscillation ( ) is given in eq.۱۰ = = . ( ) (۱۰)

۲۵. ۲۵. ۱۷ Figure ۱۰: (a) The ۵۵۵ timer connected to implement an astable multivibrator. (b) Waveforms of the circuit in (a). The duty cycle ( ) is determined using eq.۱۱ = (۱۱) In this case the duty cycle will always be greater than ۵۰٪.[۵] In our project we need the duty cycle to be ۵۰٪ so that the charging time equals the discharging time. This can be achieved by eq.۱۲ Using = Placing diode across = . ( ) (۱۲) In our design: Table ۴: Design calculations = = ۷۵۰Ω = ۰.۱ = ۱۲ = ۹.۶ Output voltage will swing between ۴ ۸

۲۶. ۲۶. ۰.۱۲ ms ۴ v wer ۱۸ Using OrCAD simulation: = ۱۲۰ = ۱ = ۸.۳۳ freque ncy = ۴ P o s pect Output ۱ swing between ۴ ۸ Output ۲ swing between −۲ ۲ Figure ۱۱: Schematic circuit of ۵۵۵timer with its voltage graph r al de nsi As shown in figure ۱۱, a coupling capacitor was added to the output of ۵۵۵timer. A coupling capacitor is used to connect between two circuits. It only passes the AC signal and blocks the DC signal.[۶] t y

۲۷. ۲۷. ۱۹ Hardware results: = ۱۰۱ = ۹.۹ = ۴ Figure ۱۲: The output signal of ۵۵۵timer on the oscilloscope Figure ۱۲ shows the actual obtained signal on the oscilloscope. It satisfies the desired goals of the designed triangular wave generator subsection. Hereby, we move to another section. ۴.۲.۲ Noise Generator In this project the jamming system needs a certain type of noise to cover a portion band of spectrum, so the most applicable type of noise in this case is the white noise. The noise in general can be defined as a Random movement of charges or charge carriers in an electronic device generates current and voltage that vary randomly with time. White noise is a random signal (or process) with a flat power spectral density. In other words, the signal's power spectral density has equal power in any band, at any centre frequency, having a given bandwidth. White noise is considered analogous to white light which contains all frequencies. An infinite bandwidth, white noise signal is purely a

۲۸. ۲۸. theoretical construction. By having power at all frequencies, the total power of such a signal is infinite. ۲۰ Figure ۱۳: Ideal white noise power spectral density In practice, a signal can be "white" with a flat spectrum over a defined frequency band. Our noise generator is based on the phenomenon of avalanche noise generated by operating a Zener diode in its reverse breakdown region. Operating in the reverse mode causes what is called avalanche effect, which causes wide band noise. The noise generator circuit consists of a ۶.۸ V Zener diode with a small reverse Current. This noise is then amplified and used in our system. We use two amplification stages: First stage, we use NPN transistor as common emitter Second stage, we use the LM۳۸۶ IC. [۴] Circuit used Figure ۱۴: Schematic diagram of the noise generator in IF section

۲۹. ۲۹. ۲۱ Spectrum analyzer output: Figure ۱۵: Noise generator output on spectrum analyzer From the results shown in figure ۱۵ we see that the implemented noise generator satisfies the desired functionality. So, we can successfully continue the jamming design process. ۴.۲.۳ Mixer Mixer is a nonlinear circuit that combines two signals in such away to produce the sum and difference of the two input frequencies at the output. The mixer here is just an amplifier that operates as a summer. So, the noise and triangular wave will be added together before entering the VCO. The LM۷۴۱ IC was used to achieve this. We need to amplify the noise signal so we took = ۱ Ω and we need the tuning signal to have the same ratio so we took = ۲ Ω

۳۰. ۳۰. ۲۲ Figure ۱۶: LM۷۴۱ Summer circuit The output signal as in eq.۱۳ = −(+ ۲ ∗) (۱۳) Hardware results: Figure ۱۷: The hardware results of the mixer circuit on the oscilloscope As figure ۱۷ shows the stability of the mixer circuit which contribute to continue our design in the same manner.

۳۱. ۳۱. ۴.۲.۴ Clamper A clamping circuit is used to place either the positive or negative peak of a signal at a desired level. The dc component is simply added or subtracted to/from the input signal. The circuit will be called a positive clamper, when the signal is pushed upward by the circuit. When the signal moves upward, as shown in figure ۱۷, the negative peak of the signal coincides with the zero level. ۲۳ Figure ۱۸: Positive clamper illustration The input of the VCO must be bounded from ۰ to ۴ V to get the needed frequency range. So, we need to add a positive clamper circuit to get our goal (as the output from the ۵۵۵timer had a DCoffset). The clamper consists of a capacitor connected in series with a resistor and diode. Figure ۱۹: Positive clamper circuit

۳۲. ۳۲. The shape of the waveform will be the same, but its level is shifted either upward ۲۴ or downward There will be no change in the peak-to-peak value of the waveform due to the clamping circuit. There will be a change in the peak and average values of the waveform. The values for the resistor R and capacitor C should be determined from the time constant equation of the circuit, t = RC. The values must be large enough to make sure that the voltage across the capacitor C does not change significantly during the time interval the diode is non-conducting. In a good clamper circuit, the circuit time constant t = RC should be at least ten times the time period of the input signal voltage.[۷] So we took the value of = ۰.۱ , = ۱۰۰ Ω , = = ۰.۰۱ = ۱۰ = ۱۰۰ = ۱۰۰ Figure ۲۰: Clamper circuit design

۳۳. ۳۳. ۲۵ Figure ۲۱: IF Section complete schematic diagram

۳۴. ۳۴. ۲۶ ۴.۳ RADIO FREQUENCY (RF) SECTION Radio frequency (RF) is a rate of oscillation in the range of around ۳ kHz to ۳۰۰ GHz, which corresponds to the frequency of radio waves, and the alternating currents which carry radio signals. Figure ۲۲: RF Section block diagram This is the most important part of the Jammer. The components of the RF Section are as follows: Table ۵: RF Section components Voltage Controlled Oscillator Crystek VCO Power Amplifier Hitachi PF۰۸۱۰۹B Antenna Omni-directional antenna The selection of these components was based on the specification of the jammer such as Desired frequency range Coverage area All the components used have ۵۰ Ω output impedance, so a ۵۰ Ω microstrip was used for component matching. The width of the microstrip was calculated using the Advanced Design System (ADS) LineCalc.

۳۵. ۳۵. ۴.۳.۱ Voltage Controlled Oscillator A voltage-controlled oscillator or VCO is an electronic oscillator whose oscillation frequency is controlled by a voltage input. The applied input voltage determines the instantaneous oscillation frequency. It is the heart of the RF-section. It is the device that generates the carrier for the noise signal which will interfere with the cell phone. The output of the VCO has a frequency which is proportional to the input voltage, thus, we can control the output frequency by changing the input voltage. When the input voltage is DC, the output is a specific frequency, while if the input is a triangular waveform, the output will span a specific frequency range. So we choose to have a tunable VCO to sweep over the range of frequencies and cover the whole band. In our design, we need to find a VCO for GSM ۹۰۰ and DCS ۱۸۰۰. There are three selection criteria for selecting a VCO for this application ۲۷ It should cover the bands that we need. It should run at low power consumption. Moreover, we need to minimize the size of GSM-jammer. So, we started to search through the internet for VCO's that work for GSM ۹۰۰ & GSM ۱۸۰۰ bands. We found the following VCO IC's Table ۶: VCO Specifications CVC۰۵۵CL CVC۰۵۵BE GSM ۹۰۰ DCS ۱۸۰۰ Output frequency is ۸۳۰-۹۷۰MHz Output frequency is ۱۷۸۵-۱۹۰۰MHz Tuning Voltage=۰.۵ to ۴.۵ v Tuning Voltage=۰.۳ to ۴.۷ v Output power is up to ۷dBm Output power is up to ۵dBm

۳۶. ۳۶. ۲۸ VCO Tuning Curve From datasheet of CVCO۵۵BE From datasheet of CVCO۵۵CL Figure ۲۳: Tuning curves of CVCO۵۵CL & CVCO۵۵BE

۳۷. ۳۷. ۲۹ We choose the ICs of all the design for the following reasons: Surface mount, which reduces the size of product. Having large output power that reduces the number of amplification stages that we need. Having same value of power supply which is typically equal to ۵ volt. Having same noise properties. ۴.۳.۲ Power Amplifier An RF power amplifier is a type of electronic amplifier used to convert a low-power radio-frequency signal into a larger signal of significant power, typically for driving the antenna of a transmitter. Since ۵dBm output power from the VCO does not achieve the desired output power of the GSM jammer, we had to add an amplifier with a suitable gain to increase the VCO output to ۳۴dBm. Figure ۲۴: PF۰۸۱۰۹B IC Power amplifier requirements ۱. Output power should be around ۳۴dBm ۲. Operating frequency in the specified band We found the power amplifier PF۰۸۱۰۹B meets our requirements and available in an old nokia mobile phones. The PF۰۸۱۰۹B Has high gain of ۳۵dB. As datasheets illustrated that this IC Is designed to work in dual band GSM & DCS

۳۸. ۳۸. Output power relation with frequency from the datasheet for both GSM and DCS For GSM ۳۰ Figure ۲۵: The output power vs. frequency curve of the PF۰۸۱۰۹B in GSM For DCS Figure ۲۶: The output power vs. frequency curve of the PF۰۸۱۰۹B in DCS

۳۹. ۳۹. ۳۱ Power amplifier gain from the datasheet for both GSM and DCS For GSM Figure ۲۷: Input power vs. output power curve in PF۰۸۱۰۹B for GSM For DCS Figure ۲۸: Input power vs. output power curve in PF۰۸۱۰۹B for DCS

۴۰. ۴۰. ۴.۳.۳ Antenna A proper antenna is necessary to transmit the jamming signal. In order to have optimal power transfer, the antenna system must be matched to the transmission system. In this project, we used two ۱/۴ wavelength monopole antennas, with ۵۰ Ω input impedance so that the antennas are matched to the system. We used monopole antenna since the radiation pattern is omni-directional.[۸] Antenna Specifications ۳۲ Table ۷: Antenna Specifications The GSM Antenna The DCS Antenna Frequency: ۸۵۰MHz-۱GHz Frequency: ۱۷۰۰-۱۹۰۰MHz Input impedance ۵۰ < ۲ We used dual band antenna for both GSM and DCS.

۴۱. ۴۱. ۳۳ Figure ۲۹: RF section complete schematic diagram

۴۲. ۴۲. ۳۴ Figure ۳۰: Jammer complete schematic diagram

۴۳. ۴۳. ۳۵ C h a p t e r F i v e ۵ RESULTS & ANALYSIS Presented By:- ۱- Abdallah Mahmoud ۲- Joumana Mohamed ۳- Mohamed Atef ۴- Suzy Sayed After we completed the implementation of our circuit and got the hardware results, we have to declare some important points: The implementation of our PCB is completed by using FR-۴ substrate with two layers. We needed to calculate the width of the transmission line in RF section in order for the circuit to work properly and match the components impedance (۵۰Ω). [۹] For that, we used ADS software, LineCalc feature, to calculate the width which was equal to ۲.۷۲ mm. After the hardware was implemented, we noticed that the power amplifier in the RF section is overheated during the circuit operation. So, it was supposed to place a heat sink underneath it to avoid that. We got the RF components from 'Mouser' company in US, as they are not available in local market. Meanwhile, the IF components were all available in local market. We were not able to simulate the RF section's results, as the components' libraries were not available in any CAD tool.

۴۴. ۴۴. We noticed in the hardware implementation testing that the jamming distance changed from that of the analytical computed one. We calculated the distance for GSM worst case scenario using the maximum frequency of the targeted band as well. As the power received from the BTS decrease, the jamming distance would increase. So, in real life, we expect the jamming distance would increase to more than ۲۰ m for GSM. ۳۶

۴۵. ۴۵. ۳۷ PCB Layout Top Layer Figure ۳۱: PCB top layer layout

۴۶. ۴۶. ۳۸ Bottom Layer Figure ۳۲: PCB bottom layer layout

۴۷. ۴۷. ۳۹ Figure ۳۳: Jammer PCB

۴۸. ۴۸. ۴۰ Jamming Test a- Obtained Spectrum Results: Figure ۳۴: Output of the jammer's VCO at GSM ۹۰۰ Figure ۳۵: Output of the jammer's VCO at DCS ۱۸۰۰ Figure ۳۴ and Figure ۳۵ show the results of the spectrum analyzer taken from the VCOs in GSM and DCS frequency ranges. The results were taken from the VCOs as the spectrum analyzer we used has a limit to the input power up to ۳۰ dBm. The resulting peak power is due to the attenuation in the device which reaches ۱۰ dB. So, the results differ from the designed one.

۴۹. ۴۹. ۴۱ b- Practical Jamming Test: Table ۸: Jammer effect's on Mobinil network's signal Mobinil Jammer OFF Jammer ON Table ۹: Jammer effect's on Vodafone network's signal Vodafone Jammer OFF Jammer ON The tables (۸) and (۹) show the status of the mobile. It can be clearly seen that the signal is "ON" when the jammer is "OFF", while the signal disappears when the jammer is "ON". This test was applied on the two operators Mobinil and Vodafone.

۵۰. ۵۰. ۴۲ C h a p t e r S i x ۶ CONCLUSION & FUTURE WORK Presented By:- ۱- Abdallah Mahmoud ۲- Joumana Mohamed ۳- Mohamed Atef ۴- Suzy Sayed In this project, which turned out to be a full success, we designed a device that stops phone ringing. This device could be used in places where ringing is not desired at specific times, as these ringings may disturb people in such places. The designed device works in dual band. It jams both the GSM ۹۰۰ and GSM ۱۸۰۰ bands. The device was able to jam the two main cell phone carriers in Egypt. We, as a team, learned more about the mobile phone's structure as the jammer components are similar to its architecture. We also knew more about the different frequency bands used in the mobile communication (GSM ۹۰۰ – DCS ۱۸۰۰). The project was implemented according to the following plan: We started by realizing how mobile jammer works and legal issues concerning using it. We studied jamming techniques to choose the best type that could match our aim. We illustrated each stage using block diagrams to clarify the concept concerning each section. We searched for components that are needed for building this device, and specified the main components which were :

۵۱. ۵۱. For the IF section, we used ۵۵۵timer, Zener diode, mixer, PC power supply ۴۳ and some discrete components (resistors and capacitors). For RF section, we needed two VCO's that operate at the needed bands, two power amplifier, and two antennas. The schematic was drawn using OrCAD design software and PCB was built using OrCAD Layout. Design test was performed either by using simulation or using experiments as libraries of most of the components were not available Some IF section simulations were performed and some were tested. RF section components were not simulated but selected based on the datasheet and performance of each component. All the IF-components were bought from local companies. Then, the IF-section was built and tested. Some RF-components (VCO) were bought from Mouser Company. Others were taken from old used mobile phones. Finally we assembled and tested the jammer. Fortunately, we got positive results. Both bands were fully jammed. Future Work: Smart jamming: jammer could be done using microcontrollers and computers. Jamming using frequency synthesizer: it jams the signal only at specific frequency by tuning the synthesizer and calculating some equations.

۵۲. ۵۲. ۴۴ REFERENCES [۱] http://electronics.howstuffworks.com/cell-phone-jammer.htm [۲] RABC M&PC Committee, "Use of Jammer and Disabler Devices for Blocking PCS, Cellular and Related Services", [online]. Available: http://www.rabc.ottawa.on.ca/ [۳] RICHARD A.POISEL, "Modern Communications Jamming Principles and Techniques", ARTECH House, ۲۰۰۴. [۴] S. Shah, S. Zafar, and S. Jafri, "GSM Jammer", ۲۰۰۶. [۵] A. Sedra, K. Smith, "MICROELECTRONIC CIRCUITS", OXFORD UNIVERSITY PRESS, ۲۰۰۴ [۶] http://www.learningaboutelectronics.com [۷] http://www.circuitstoday.com/diode-clamping-circuits [۸] K. Siwiak, Radio-wave propagation and Antennas for personal communication. [۹] D. Pozar, "Microwave Engineering, John Wiley and Sons", ۲۰۰۵.

۵۳. ۵۳. ۴۵ APPENDIX

۵۴. ۵۴. ۴۶

۵۵. ۵۵. ۴۷

۵۶. ۵۶. ۴۸

۵۷. ۵۷. ۴۹

۵۸. ۵۸. ۵۰

۵۹. ۵۹. ۵۱

۶۰. ۶۰. ۵۲

۶۱. ۶۱. ۵۳

۶۲. ۶۲. ۵۴

۶۳. ۶۳. ۵۵

۶۴. ۶۴. ۵۶

۶۵. ۶۵. ۵۷

۶۶. ۶۶. ۵۸

۶۷. ۶۷. ۵۹

۶۸. ۶۸. ۶۰

۶۹. ۶۹. ۶۱

۷۰. ۷۰. ۶۲

۷۱. ۷۱. ۶۳

۷۲. ۷۲. ۶۴

۷۳. ۷۳. ۶۵

۷۴. ۷۴. ۶۶

۷۵. ۷۵. ۶۷

۷۶. ۷۶. ۶۸

۷۷. ۷۷. ۶۹

۷۸. ۷۸. ۷۰

۷۹. ۷۹. ۷۱

۸۰. ۸۰. ۷۲

- [GSM-۹۰۰ Mobile JAMMER](#)
  [Garry۵۴](#)

- [Cell phone detector & jammer](#)
  [Raj Malhotra](#)

- [Mobile jammer](#)
  [Avay Minni](#)

- [cell phone jammer report](#)
  [Sameer Gupta](#)

- [Intelligent jammer](#)
  [Prejith Pavanan](#)

- [Mobile Jammer report](#)
  [Mehul Ranavasiya](#)

- [English](#)
- [Español](#)
- [Português](#)
- [Français](#)
- [Deutsch](#)

- [About](#)
- [Dev & API](#)