GEEKS AND NERDS

AN EMPLOYEE-OWNED COMPANY

Hacking an "Amazon's Choice" Security System

An Introduction to RF Hacking

5 June 2019

Introduction

- **Jake Schneider – Geeks and Nerds**
  - I'm not an RF engineer
  - I am a computer scientist and a hacker
- **Dr. Hans G. Schantz – Geeks and Nerds**
  - I'm a physicist: electromagnetics, analog RF, antennas
  - I write science fiction about cybersecurity
- **Dr. Tom Sutherland – Geeks and Nerds**
  - I am an Electrical Engineer, but don't hold that against me.
  - I dabble in many things and know little about everything.
- **We will talk plainly**

GAN GEEKS AND NERDS

Agenda

- **This talk is for:**
  - STEM people
  - Curious people
  - People who just want to see a cool hack
- **We will cover:**
  - Hardware/Software tools
  - Song lyrics
  - Mathematics
  - Pretty graphs
  - Demos
  - Mitigation strategies

GAN GEEKS AND NERDS

Acronyms

- RF – Radio Frequency
- GRC – Gnu Radio Companion
- SDR – Software Defined Radio
- FCC – Federal Communications Commission
- FSK – Frequency Shift Key
- PSK – Phase Shift Key
- ASK – Amplitude Shift Key
- QAM – Quadrature Amplitude Modulation
- QPSK – Quadrature Phase Shift Key
- OOK – On Off Key

Hardware Tools

- **RF hardware is cheap and readily available**
- **HackRF One ~$300**
- **Reasonably fast computer**
  - » Demos on a 8th Gen Core i5
- **Optional**
  - » USB Thumb drive

The Target

Wireless Home Office Business Security Alarm System, GSM SIM Card Burglar Alarm Outdoor Siren, with Auto Dial, Infrared Detector, Remote Control and More Kits for Complete Security

★★★½☆ 11

$77.99

FREE Shipping

Total cost of experiment:

Laptop	$1200
HackRF	$ 300
USB drive	$ 10
Target	$ 80
	$1590

GEEKS AND NERDS

Software Tools

- **Linux**
  - » Pentoo
- **GnuRadio**
- **GnuRadio Companion (GRC)**

GNU Radio
THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

GAN GEEKS AND NERDS

Before We Start – Don't Break Laws

- **Federal Communications Commission (FCC)**
- ***"So the FCC won't let me by or let me be me so let me see."***
  - Eminem
- ***"Now if the CIA, and the IRS, and the FCC, Found out that J. Edgar Hoover and the FBI owned stock in AT&T"***
  – Charlie Daniels
- ***"To the haters, the takers, the liars, all the vultures and the bottom feeding scum, the FCC, the FBI and every tin god with a badge and a gun"***
  – Five Finger Death Punch

Photo Credit: https://www.discogs.com/

FCC (continued)

- **FCC makes RF hacking much easier**
  - » https://www.fcc.gov
  - » Every transmitter has an FCC ID
  - » Target FCC ID
- **FCC makes RF transmission at certain frequencies/power levels illegal—for good reason**
  - » Hospitals
  - » GPS & Aviation Communications
  - » Emergency services

The Attack Process

- **Find the transmit frequency (FCC website)**
- **Discover the Modulation Scheme**
  - This will require a discussion of math
    - Spoiler: Numbers are Spirals
  - We will also look at pretty graphs
- **Program our SDR**
- **Transmit our Attack**
  - Demo Time!

Security System Keyfob

Security System Base Station

HackRF One SDR

FCC ID

- No FCC IDs found
- Logo on the box
- Probably not supposed to be sold in the US
- FCC.gov is un-navigable
- FCC.io is great!

FCC ID for my Vehicle

10 Matches found for FCC ID CWTWB1U840

View Attachment	Exhibit Type	Date Submitted to FCC	Display Type	Date Available
Special Power of Attorney	Cover Letter(s)	02/15/2012	pdf	02/15/2012
Authorization Letter	Cover Letter(s)	02/15/2012	pdf	02/15/2012
Request for confidentiality letter	Cover Letter(s)	02/15/2012	pdf	02/15/2012
Request for short-term confidentiality letter	Cover Letter(s)	02/15/2012	pdf	02/15/2012
External Photo	External Photos	02/15/2012	pdf	08/13/2012
Label Drawing and Location	ID Label/Location Info	02/15/2012	pdf	02/15/2012
Internal Photo	Internal Photos	02/15/2012	pdf	08/13/2012
Test report	Test Report	02/15/2012	pdf	02/15/2012
Test setup photo	Test Setup Photos	02/15/2012	pdf	08/13/2012
User Manual	Users Manual	02/15/2012	pdf	08/13/2012

FCC provides all this useful information for free download!

GAN GEEKS AND NERDS

Quick Hack

- **Actually, you don't have to understand much of anything.**
  - » Common consumer frequencies are easy enough to scan (315 MHz, 433 MHz, 900 MHz, 2.4 GHz, etc.)
  - » Let's do a replay attack!
- **hackrf_transfer –r NCS433.raw –s 20000000 –b 5000000**
- **hackrf_transfer –t NCS433.raw –s 20000000 –b 5000000 –a 1 –x 40**

Demo Video

That Shouldn't have worked!

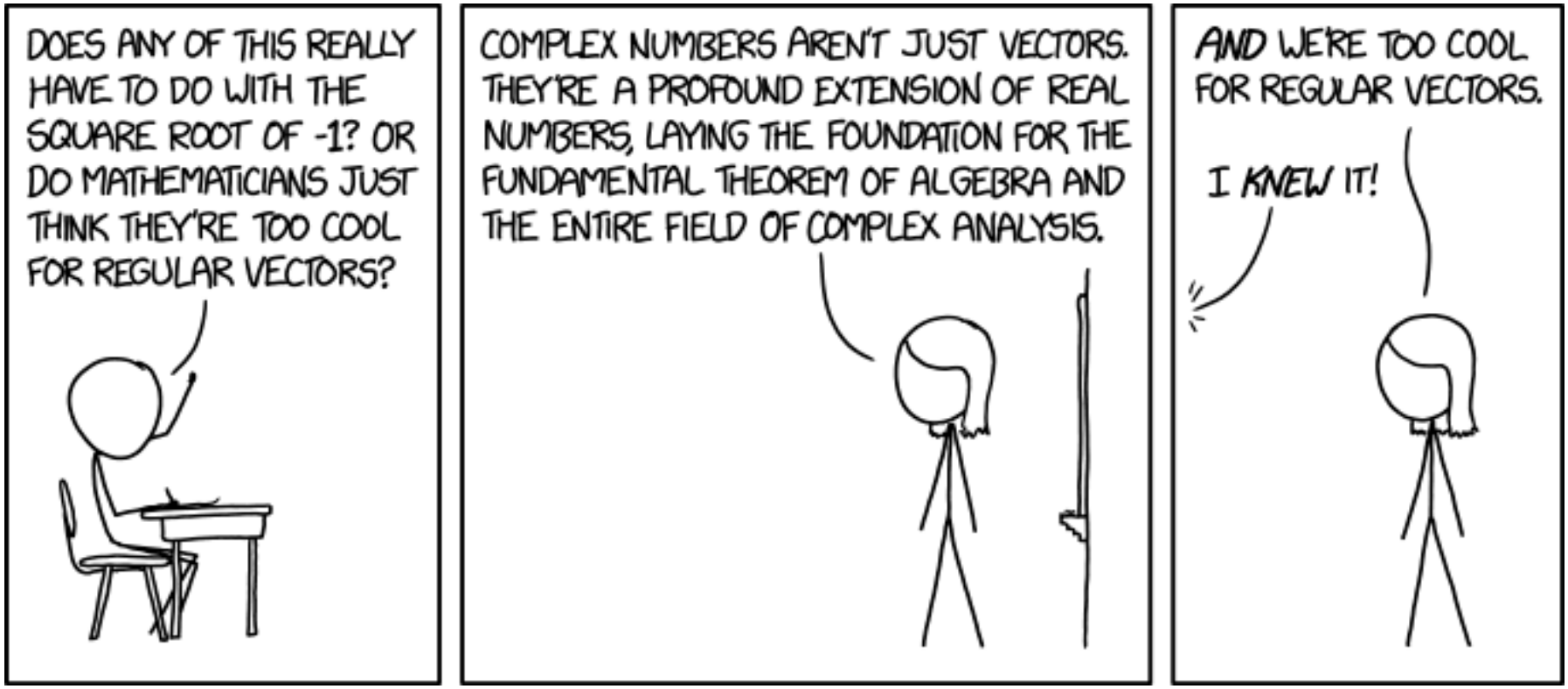
GIF Credit: https://giphy.com/gifs/captain-facepalm-picard-XsUtdIeJ0MWMo

Advanced Attack Techniques

- **Generative attacks**
  - Ways to control the target

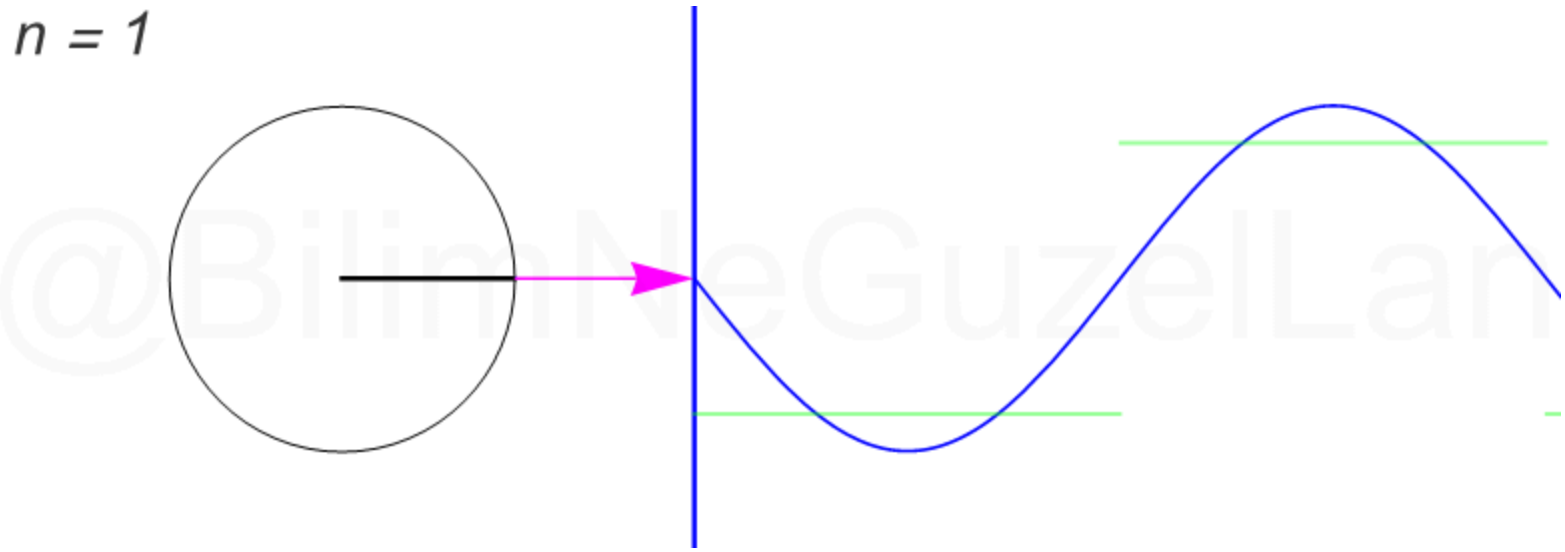
Imaginary/Complex Numbers

- **Remember complex numbers?**
  - » That's OK, I'll teach them to you in 1 minute



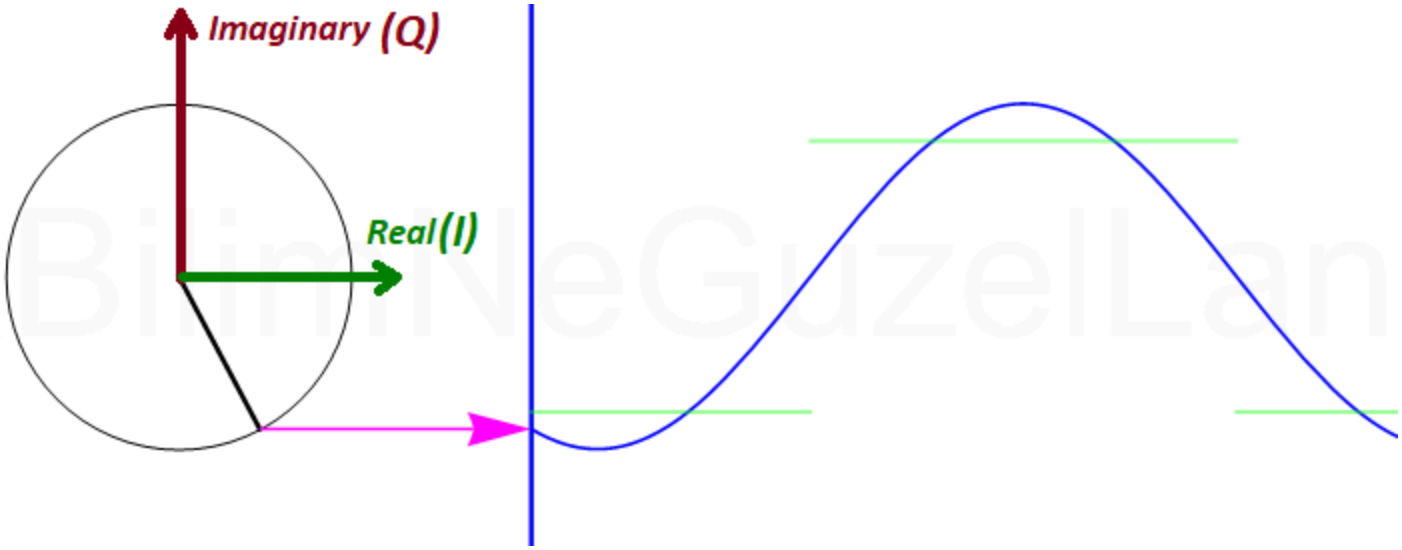
Credit: https://xkcd.com/2028/

Complex Numbers Explained Visually

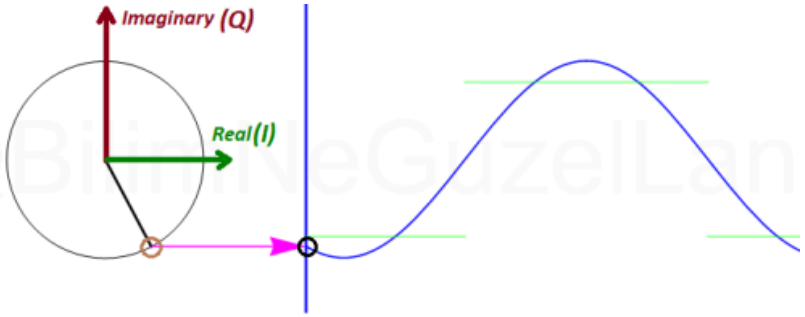


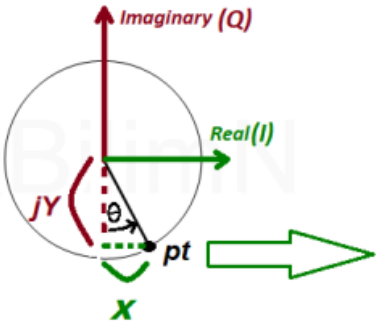
Credit: http://bilimneguzellan.net/fuyye-serisi/

Complex Numbers Explained Visually



Complex Numbers Explained Visually





Any point on a sinewave can be represented as a complex number.

$$pt = X + jY$$
$$= 1 \cdot \cos\theta + j \cdot (-1) \cdot \sin\theta$$
$$= \cos\theta - j\sin\theta$$

$$e^{j\theta} = \cos\theta + j\sin\theta$$

"Eulers Identity"

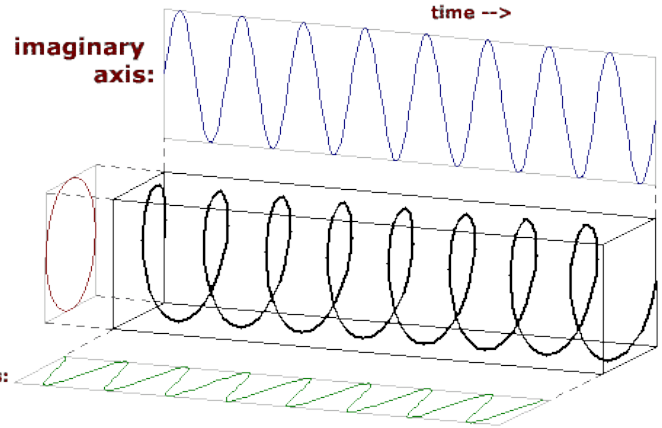
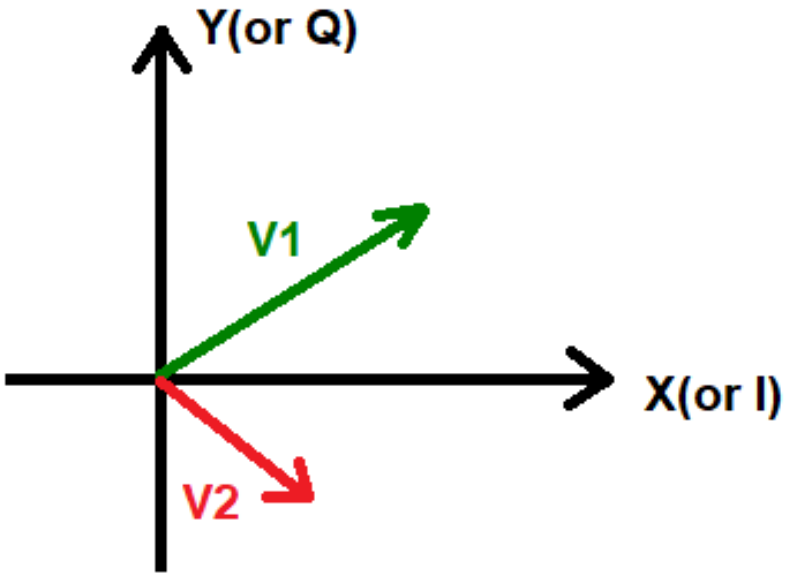
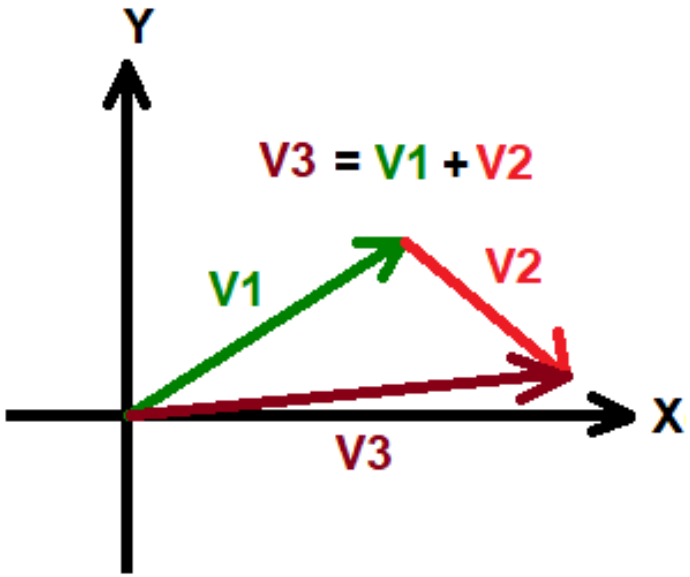


Image credit: http://peabody.sapp.org/class/st1/final/answers.html
https://en.wikipedia.org/wiki/Leonhard_Euler

Complex Numbers: Vector Math

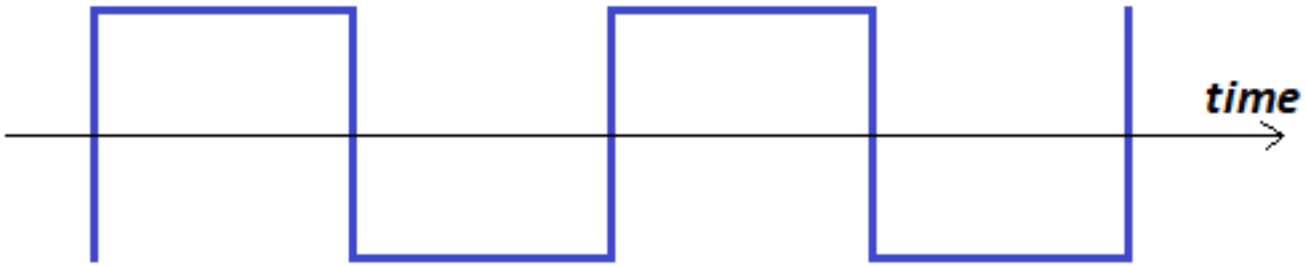




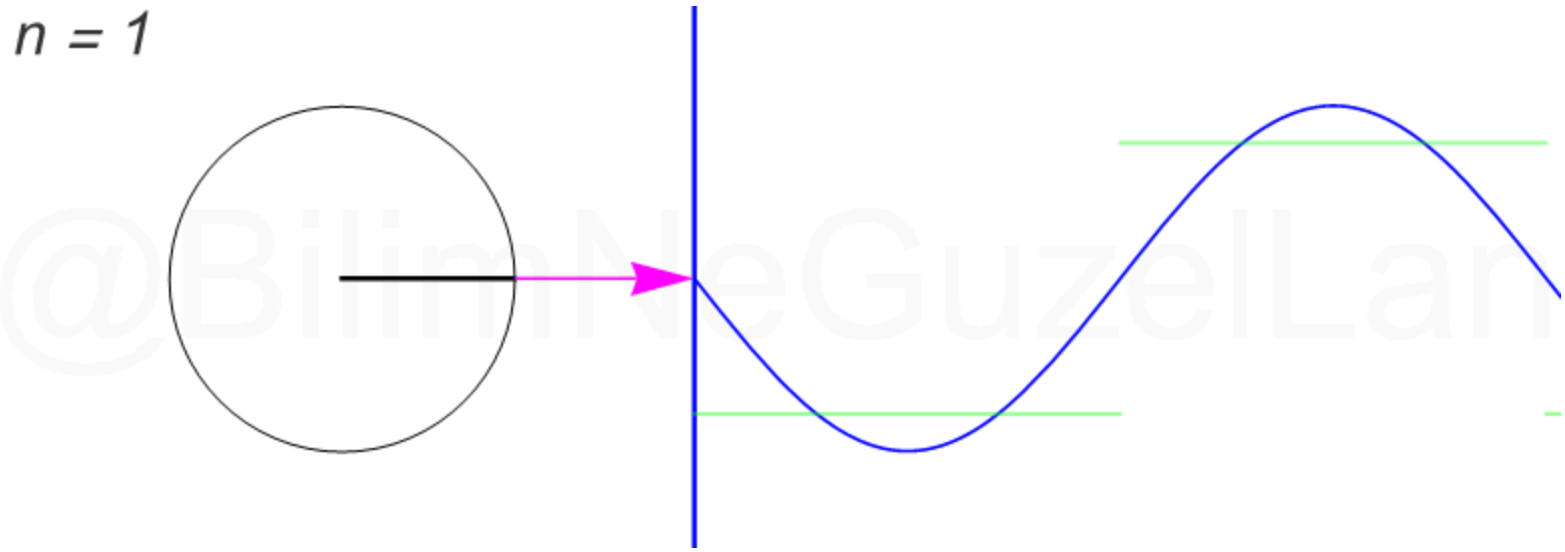
$V1 = (x1,y1)$
$V2 = (x2,y2)$

$$V3 = V1 + V2$$
$$= (x1,y1) + (x2,y2)$$
$$= (x1,x2) + (y1,y2)$$
$$= (x3,y3)$$

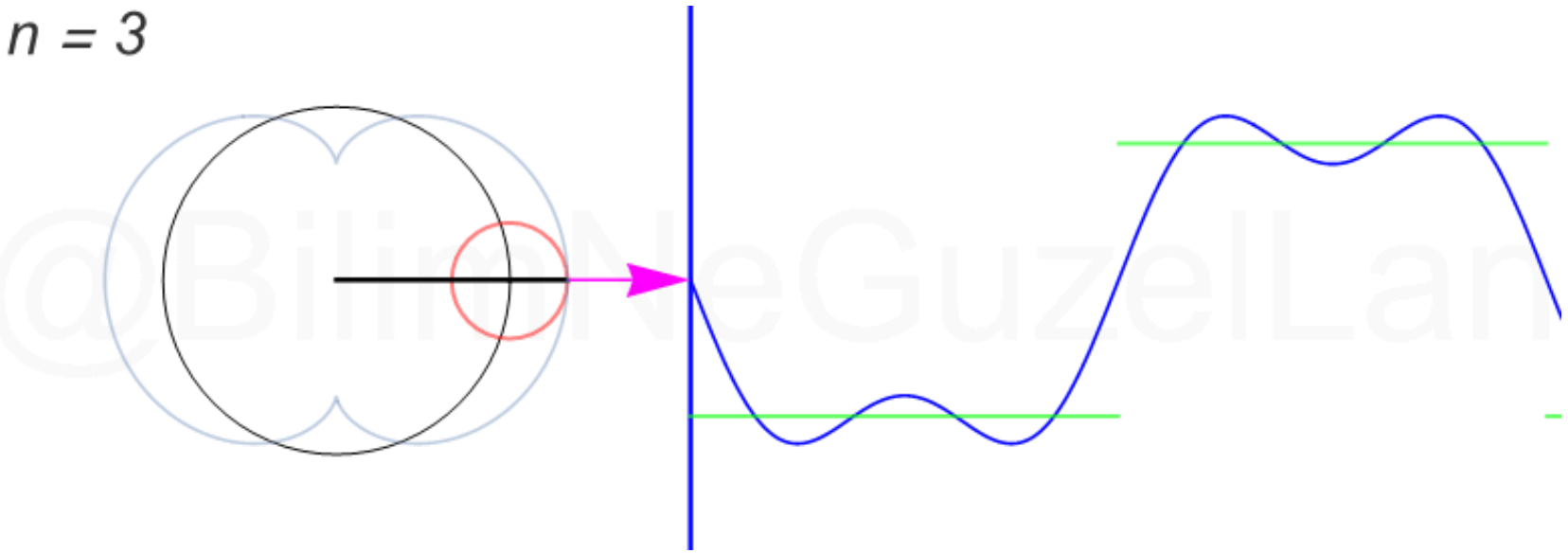
- **If we want to create a particular waveform,**
  - Example: Square Wave



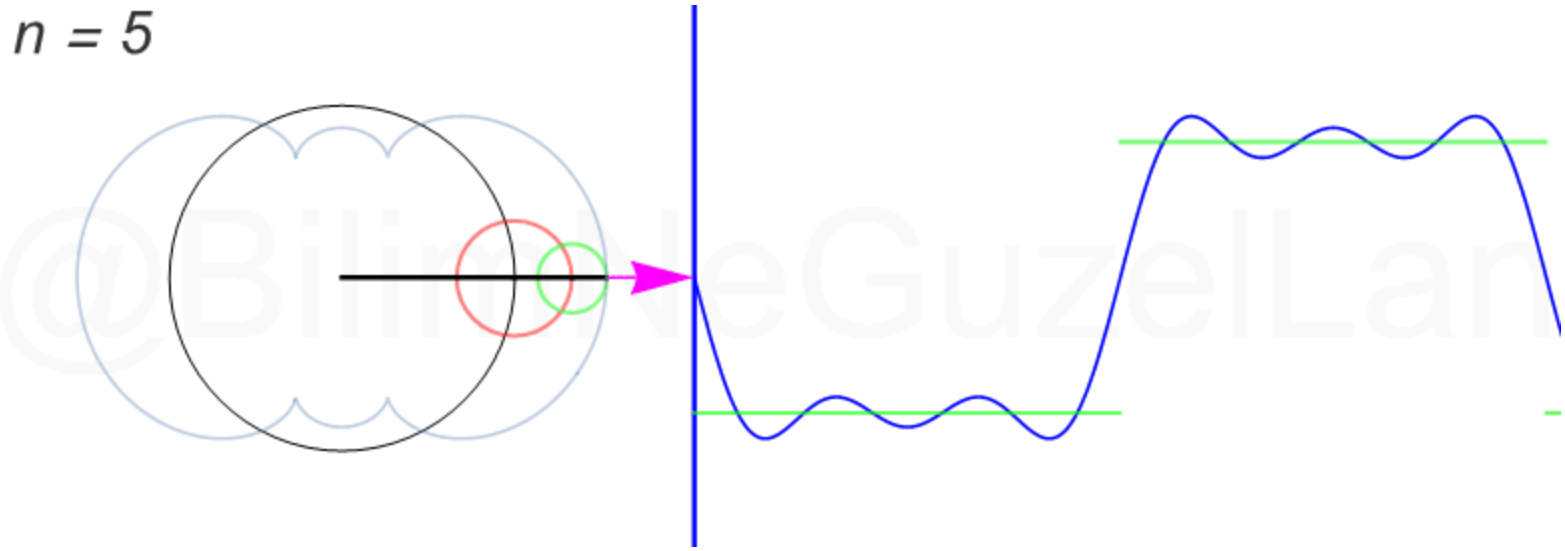
Complex Numbers Explained Visually



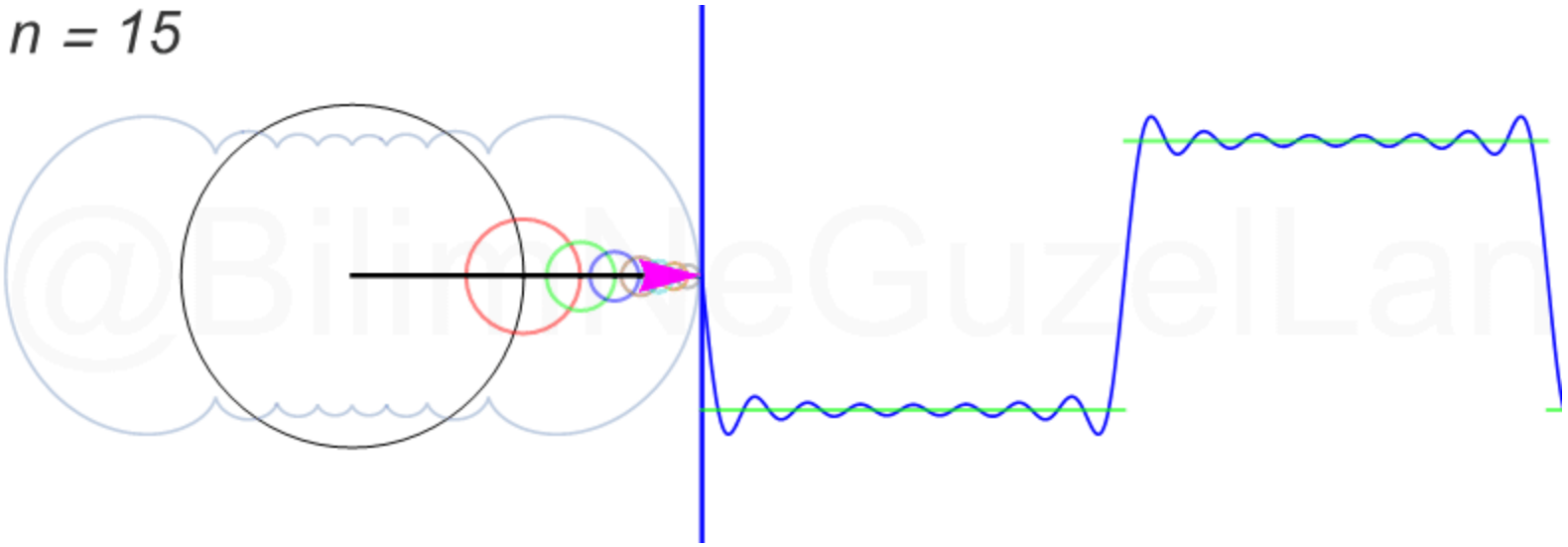
Credit: http://bilimneguzellan.net/fuyye-serisi/



Credit: http://bilimneguzellan.net/fuyye-serisi/



Credit: http://bilimneguzellan.net/fuyye-serisi/

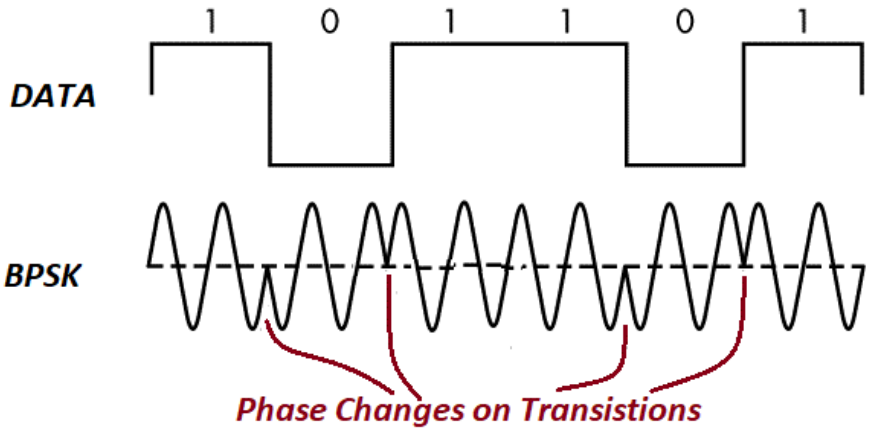


Credit: http://bilimneguzellan.net/fuyye-serisi/

- Any arbitrary waveform can be created by summation of sinusoids of various frequencies.
- Lets say we are not so much interested in the waveform shape but on sending information with a waveform.
- A single sinusoid doesn't contain much information unless we turn it off-on such as Morse code. 
- If we want to transfer data, 0 & 1, how can we create a waveform that contains the data?

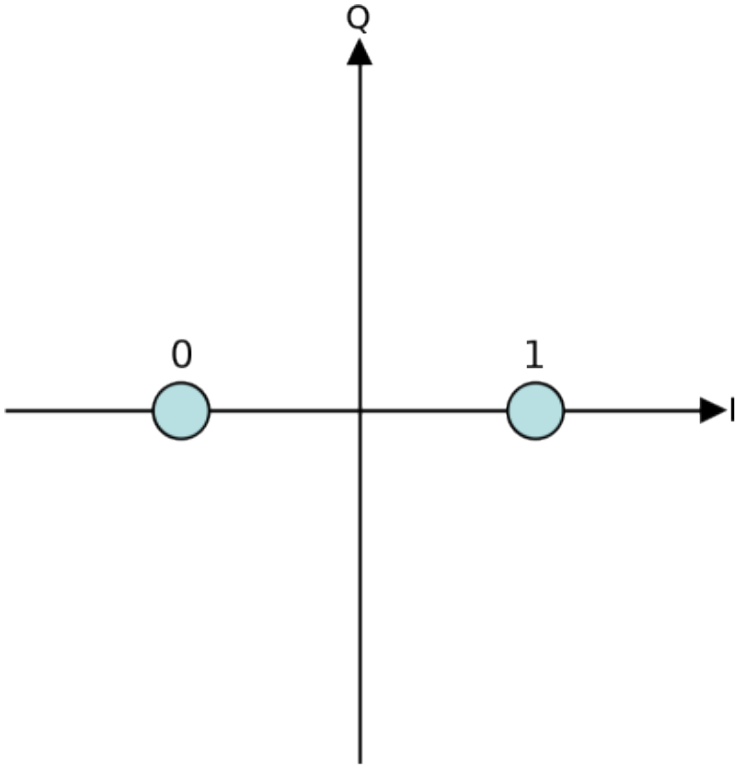
Modulation Techniques

- **One of the simplest methods to encode data is Binary phase-shift keying (BPSK).**
  - » This takes a single frequency sinusoid and calls it a bit = 1.
  - » To create a "0", you flip the phase of the sinusoid by 180°



Modulation Techniques

- A "Constellation" diagram shows the relative position of the two data bits. This is considered 1 data bit per symbol.

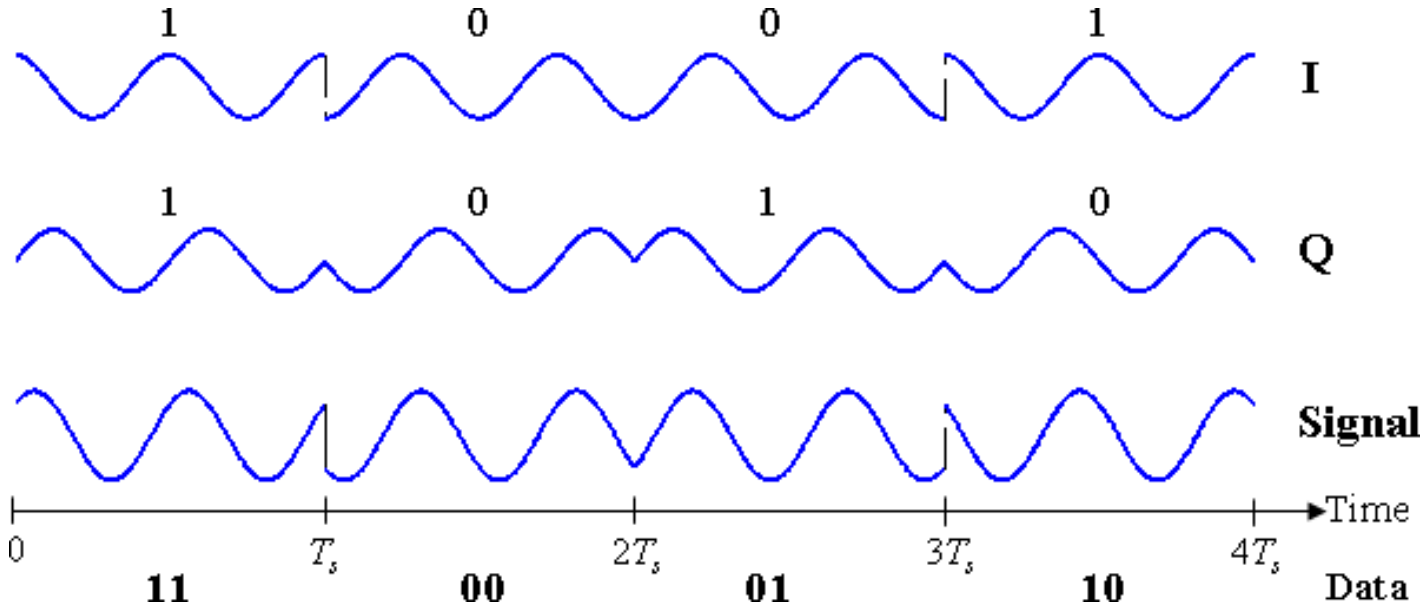


Credit: http://www.wikipedia.org

Modulation Techniques

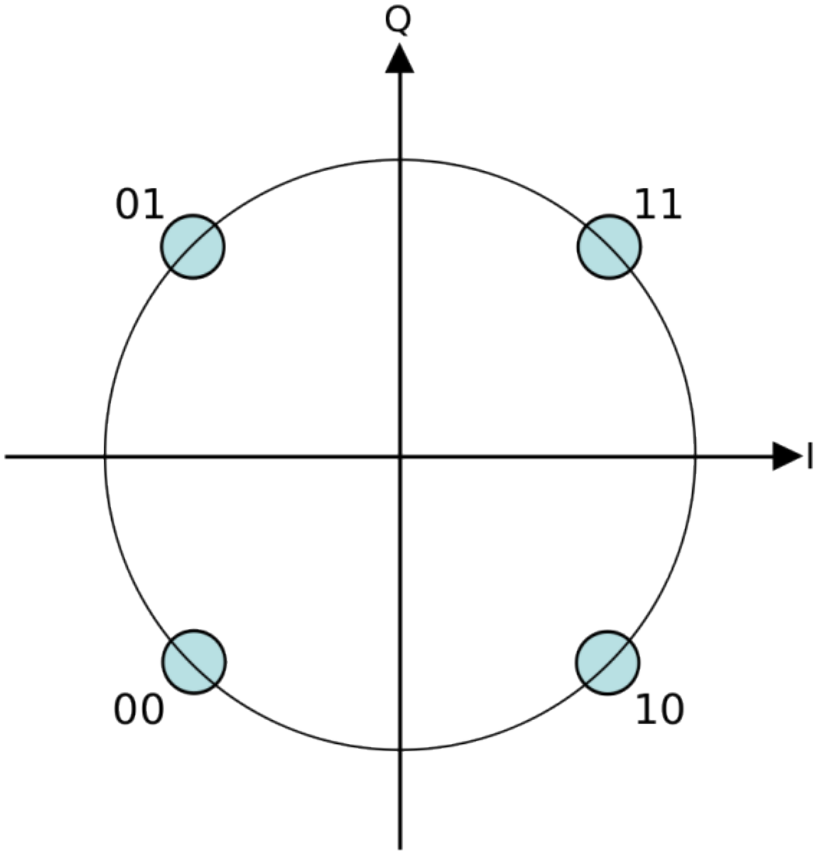
- **You can increase the number of bits per symbol (get more information encoded for the same bandwidth) by going to Quadrature phase–shift keying (QPSK).**
  - » Quadrature increases the number of bits encoded by dividing the phase shift from two possible (0 and 180°) positions to four (45°, 135°, 225° & 315°).
  - » These four positions allow for 4 different symbols to be encoded equivalent to 2-bits. (00, 01, 11, 10)
  - » The 2-bits are separated into two signal streams, I & Q, and each modulated with BPSK and then added together.

- **The two data streams and their sum:**



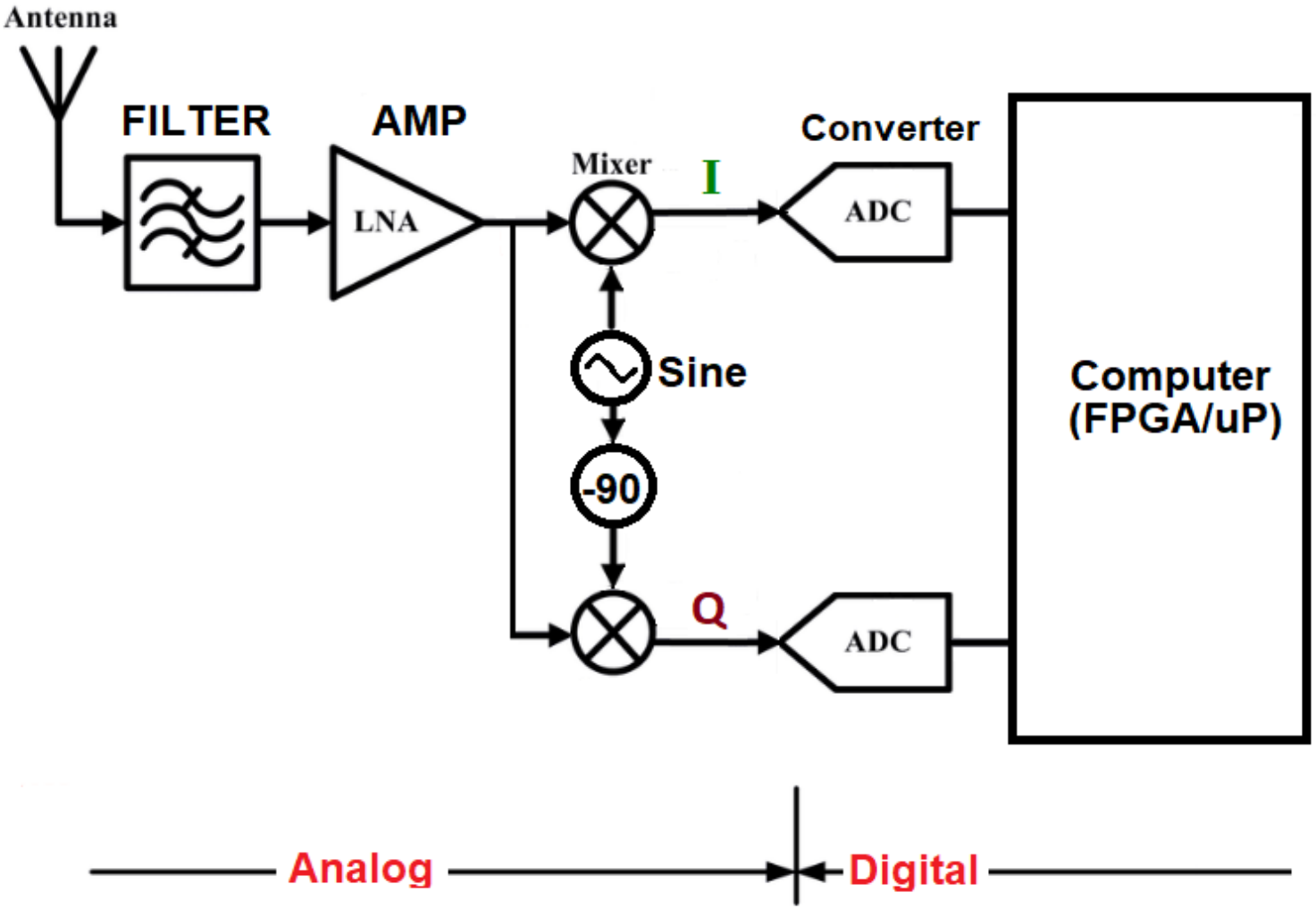
Credit: http://www.wikipedia.org

- **The "constellation" diagram for QPSK:**



Credit: http://www.wikipedia.com

Software Defined Radio (SDR)



Modulation Summary

- Modulation schemes are necessary to carry digital data over analog waveforms
- Modulation must be correct for the receiver to get your message
- Protocol analysis may be necessary to figure out message structure
- You can fuzz over RF to try things out
  - » Danger, poorly designed devices can lock up if you send the wrong data

Mitigation Strategies

► Encryption

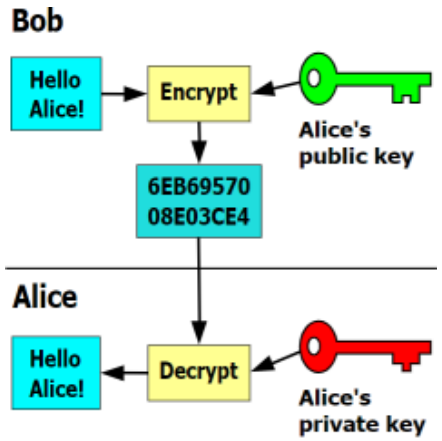
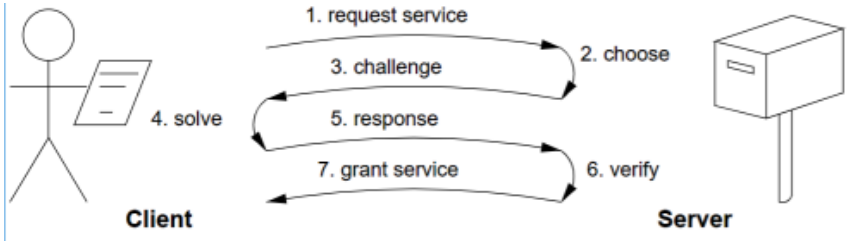


Image Credits:

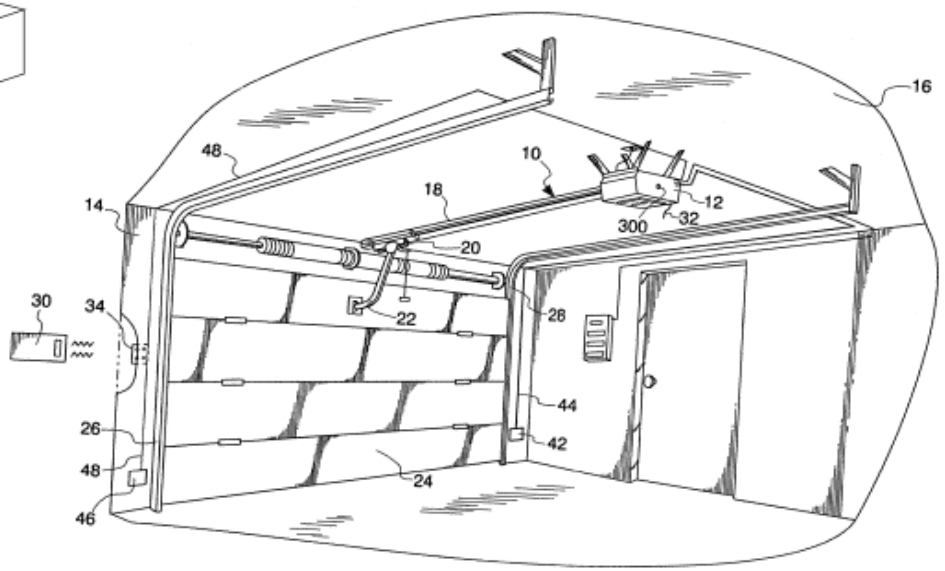
- https://upload.wikimedia.org/wikipedia/commons/f/f9/Public_key_encryption.svg
- https://upload.wikimedia.org/wikipedia/commons/5/55/Proof_of_Work_challenge_response.svg
- Patent US7412056

► Challenge/response



► Rolling codes

Patent US7412056 –
Rolling code security system



Shameless Plug

- **GaN is hiring!**
- **https://www.GeeksAndNerds.com**