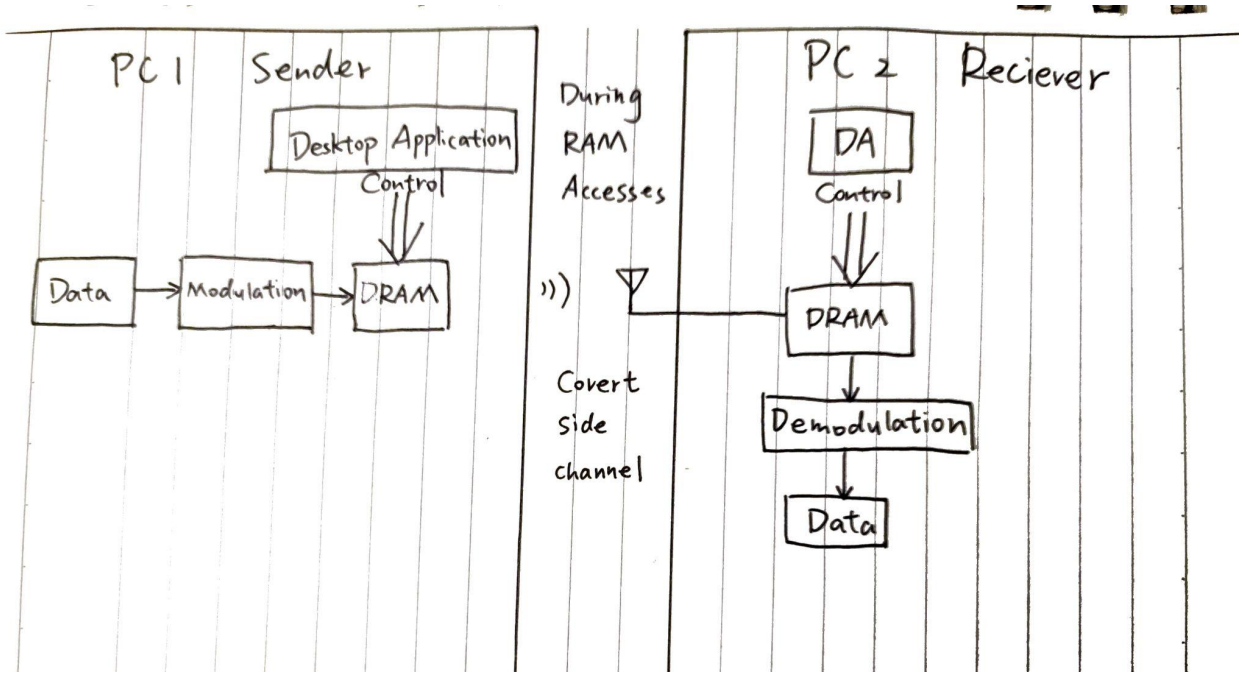
Project 6. Electromagnetic Side Channel for Data Transfer

Motivation
In modern cyber-physical systems, cache and memory accesses by the CPU result in emission of electromagnetic radiation. By carefully managing these cache and memory accesses it is possible to modulate data bits on these emitted electromagnetic radiations. Such a side-channel can be used to leak information in a covert manner.

Design goals
Develop a covert side channel for data-transfer between the desktop computers by modulating data using memory accesses

Deliverables
Write desktop application that uses DRAM accesses to modulate data over EM radiations emitted during RAM accesses
Receive EM radiations emitted by DRAM accesses on another Desktop using SDR and perform demodulation
Experimental results to demonstrate a working communication channel between the two PCs.

System blocks



Software Requirements:
Python for desktop application, Matlab for Modulation

Hardware Requirements:

Software defined radio platform, Digital Storage Oscilloscope, Waveform Generator

Team members responsibilities
Nengxing Shen: perform the signal modulation part
Mingrun Zhang: perform SDR implementation
Yaozhong Zhang: write and complete the desktop application

Project timeline
Study the materials and references of SDR,and knowledge about DSP focusing on modulation by Oct 15th.
Design the technological details of covert side channel for data-transfer and operate simulation by software by Oct 31st.
Write and implement the desktop application by Nov 15th.
Implement the channel on SDR and operate experiments to verify the designed method: Nov 30th.
Final demonstration on Dec 7th.
Project report due on Dec 16th.

References
BitJabber: The World's Fastest Electromagnetic Covert Channel
bitjabber.pdf (zhenkai-zhang.github.io)
When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient