

# Is secure communication possible?

---

Supervisors:  
Derek Abbott  
James Chappell  
Lachlan Gunn

Yuanhao Liu  
Christopher Lau

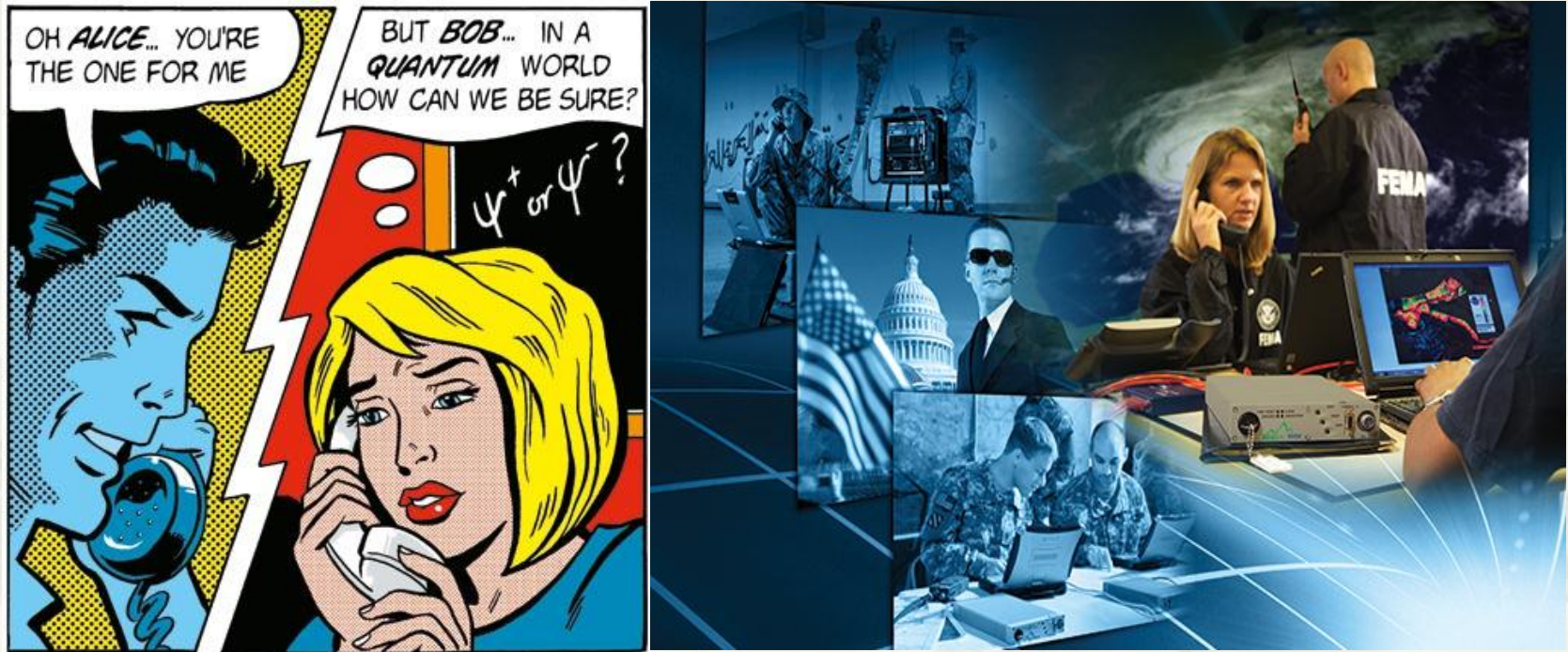
# Outline

---

- Introduction
  - Is communication secure?
  - Power of eavesdroppers
  - Importance of cryptography
- Encryption
  - One time pad
  - Round trip times
- Our aims
  - The efficiency
  - The reliable
  - The speed
  - The utilisation
- Approaches
  - Software
  - hardware
- Project management
  - Risk management
  - Time management
- Question and references

# Introduction

Is communication secure?

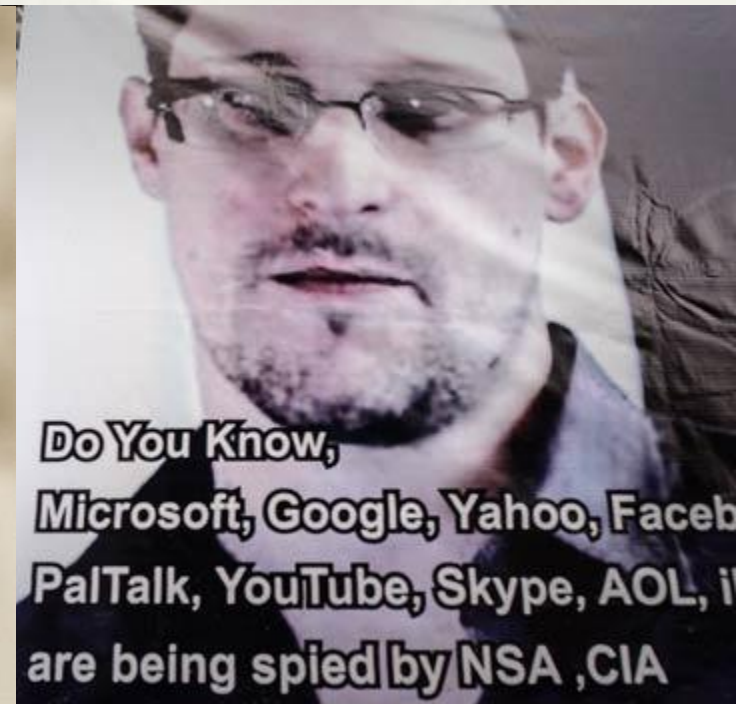


<http://physicsworld.com/cws/article/news/2013/apr/16/alice-and-bob-communicate-without-transferring-a-single-photon>, <http://www.viasat.com/information-assurance/network-security-appliances>

# Introduction

---

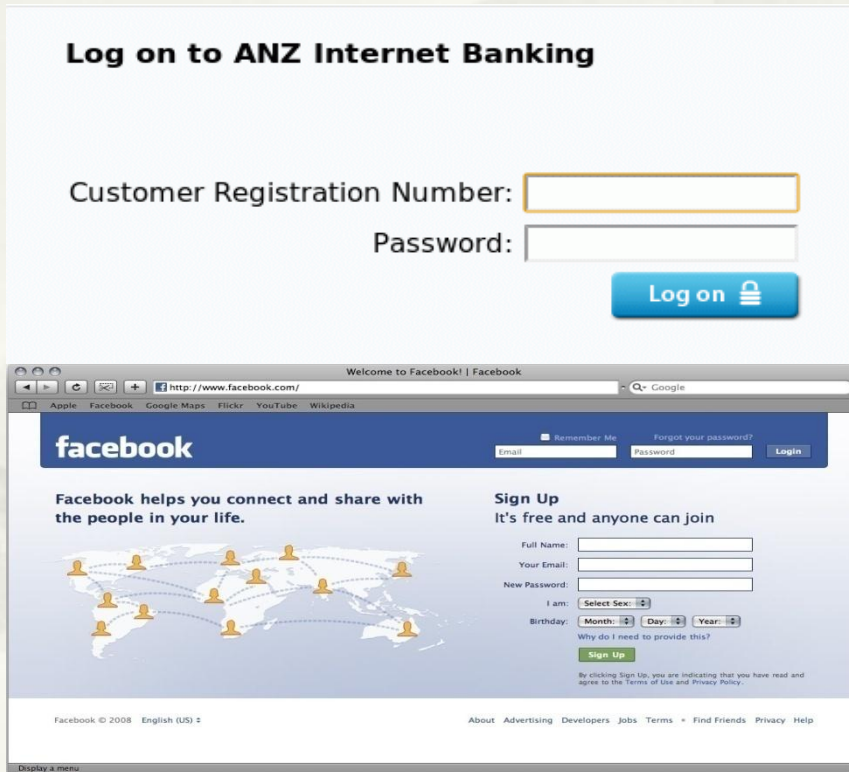
## Power of eavesdroppers



<http://blog.zap2it.com/pop2it/2013/06/nsa-leaker-edward-snowden-seeks-asylum-in-ecuador-lands-in-moscow-for-the-time-being.html>  
<http://rt.com/usa/obama-internet-wiretap-surveillance-009/>

# Introduction

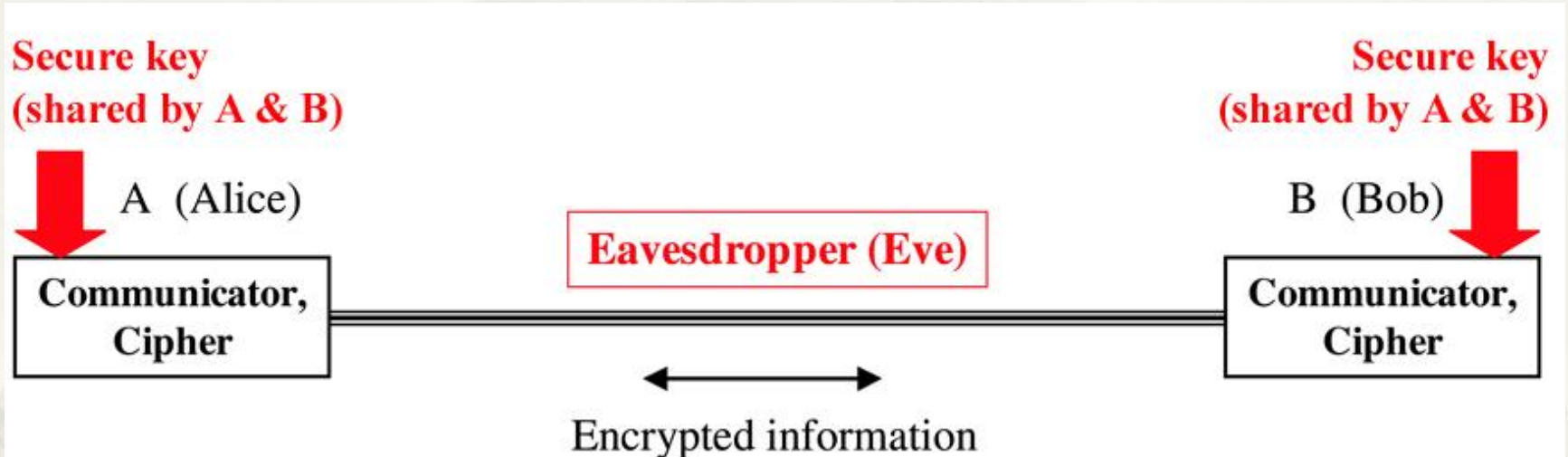
## Importance of cryptography



<http://www.lemis.com/grog/photos/Photos.php?dirdate=20131025>, <http://www.flickr.com/photos/psylum/2982646566/>, <http://alexansary.tv/george-soros-bet-1-3-billion-stock-market-will-fall/>

# Encryption

One time pad – share the key

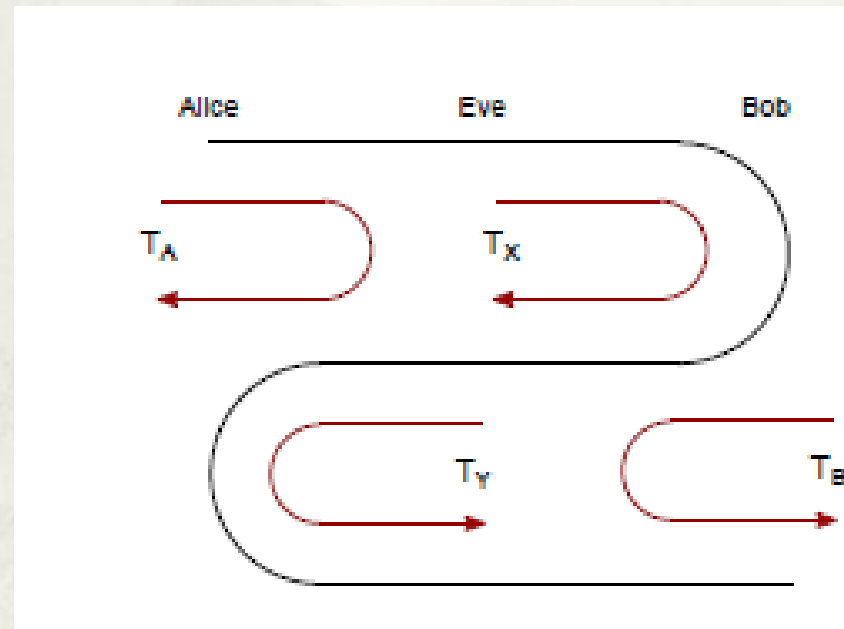
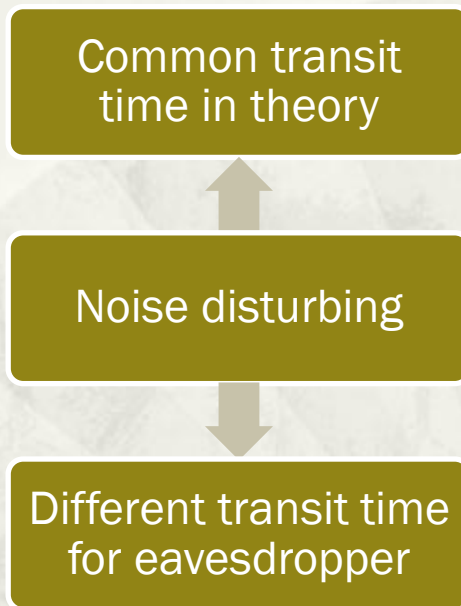


Source: <http://spie.org/x16669.xml>

- The first unbreakable cipher [1]

# Encryption

## Round trip times



Source: L. Gunn, J. Chappell, A. Allison & D. Abbott

# Timing based encryption

## Steady channel

```
A_stream2.txt vs. B-stream2.txt | A_stream3.txt vs. B-stream3.txt | A_stream4.txt vs. B-stream4.txt
161 000001011100010000001010100100110001000101000101100010000100011001101111000001 x 00000101110001000100101010010100010000110001000100100001000111011011100000001 162
162 0111000001000101001000010001100011011110000000100001001000111101001100101010 x 0100000000000010000100010001101111011010000100100001000011101001100101010 163
163 01100000101100110011011001001000001001010110110110110110110110110110110110110 x 01100100110110011001001111000110010001001001011011011011000110100010100010 164
164 11110101100001010110010101001000010110000100101010000111011011001100101011 x 000101011011010100101101101000100010011101101001011000010110010100101011 165
165 000000000101010001001100010010100100001010000100010000001000010000000001011 x 00000101010101001110101000101101000011100001110000011000011011010000010011 166
166 10000001000101011010100111011010000101000010110001000100010100001110010110 x 100000010011000101011011001100101110000001010000100010100000011100110011 167
167 1011001101100110001010100100001001010100101101011001100110011010110110001 x 1000010101000110001010100110000101010101010010110101010101010101011001 168
168 101111000101010111101010000101001100010100110001010011001010001000010101 x 10011000010010110000101010010100110010000001010011011110001011000100011011 169
169 0010111110101010010111110000000111000111001100110100110100110010010001010 x -
170 00000000111110110011101100111000110010101010101001100100110010010001010 < -
171 0000110001011000100000101000110010111100111101010010001010000000110000 x 001000011110110110000101011101000011101000011000111001101000000110010010001010 170
172 0011011011100001000001100010000101000001110000101011001010111101101111 x 001000000101110110011010100101001010011110100110010001100001111010011101 171
173 0110010110010111001101100011111001101010000111011000000101011110111011 x 00110100011111111100000000001001010111111101000001000101101000000011110 172
174 1010101110111011011011010101000001010010011100010111000101101101010111000000 < -
175 001111101110011100000100000100011111101100011100101110011110010011010111 < -
176 0001000010001001101110000111011010001010001110101011101100110111001110 < -
177 1110101010101110110000111011010001010001110101011101100110111001110 < -
178 1110101010101110110000110001110010000001100100101000000111000100100010111 < -
179 11101000100001010100010000001001100100010000000001001111010001110101 < -
180 01101000110001101110100001011010010010010101101111010100010100001 < -
181 10100101100110100010001111011110010100011110110011011101000001010001 < -
182 1110111001100000100011100000101000011100101110110011101000100101000100 < -
183 000011111001000100000000101101100010111100000000010001010101000000100010 < -
184 0100011101100000101001001110100010001110110110110111101111000010110000100 < -
185 010001010000001001100110011000100000100001101100001010000101100100010001001 x 001011000111001100010100000100000100000000001111001000010000010101111 173
186 100110011010101001011100001011000101010000101000011111101010111000110101 < x 011110010000101000100001011000111111011010100001100101000001100110011011 174
> 110010001101110001011011000101000010100000000001000101010110001011100110111 175
> 01000111011100101010001001001011111110110001111011100011101100110011001101 176
> 11010000101101101101001011111001101110000000100110111101001111110011110 177
> 11101010101111101111011010101010000111110000011000000011001010100001111 178
> 1110100010110110110001100000001100101010001000000000110110011101001110101 179
> 011100000101110010100001011010100110111011011001100110111010100010111001 180
187 1110111111000101011110111100111001011110010100000001010111001101100000 x 101000101011101000010101110111100100001010101001101111000000010100110101 181
188 111100010101110011011001010101000011000110010100000010101000010101010110 x 110001100110100000100001100000101001001011001010001111110010000001000100 182
189 00001001111001011001100010000001011110000101100110111111000000100110101 x 0000110000100010001001100010111101101111011111000000000100011010100011000010 183
190 000010010100010100000101011010111101011100100010010101110000010101100011 x 010000110100100001010010011100001010010100000110110000011001101000100000100 184
191 0000100000100100111100010010100011101011100000010100111010100000000100 x 01000010100001011000100110001001100000010100000100101110110011000000001001 185
192 10100000011010001000001010100010011001001000000011110110000101010111100 x 0101001100010101000010000001100001010101000000110000011111011000101000010111 186
193 10010110000001000010100100001110101001110010010011111111110010001000 x 010111100001010101111011010001000111111011000000010001101000001100001 187
194 0001011110000001010111000100010101011111101000101100010111000101101010 x 111100010101010010110101010011000100000000100101010110111000011010101 188
195 00000101100000011111010110101100110000001000101100101010100111001111010000 x 0000010110010101001100011110010101011001101100000010001110000001010101010 189
196 01100011010110100010000100000101100100110001100110001101111100 < x 10011000110010101011100101011101010001101111001010111000001100000110001010 190
> 000010011000111100100000111001010000101101000001001100100001101100001 191
> 101001101110000100100110101000011101101000010010101010110101000110001001 192
> 11011011000110110001010101010000111001111010010111111110101010101010101 193
> 00000110011100111001111000100100010101111000011101111001100010110101010 194
> 001010101101111001100010100101100111000100100110100000110000111100010011 195
> 011110101010100001110100000101000001010001000101010000110000111100010011 196
```

Number of matching lines: 53  
Number of unmatched lines in left file: 143  
Number of unmatched lines in right file: 143

```
>> CompareBits
The length of the two bit streams is 16054
The number of errors between the two bit streams is 917
The BER between Bob and Alice is 5.712%
```

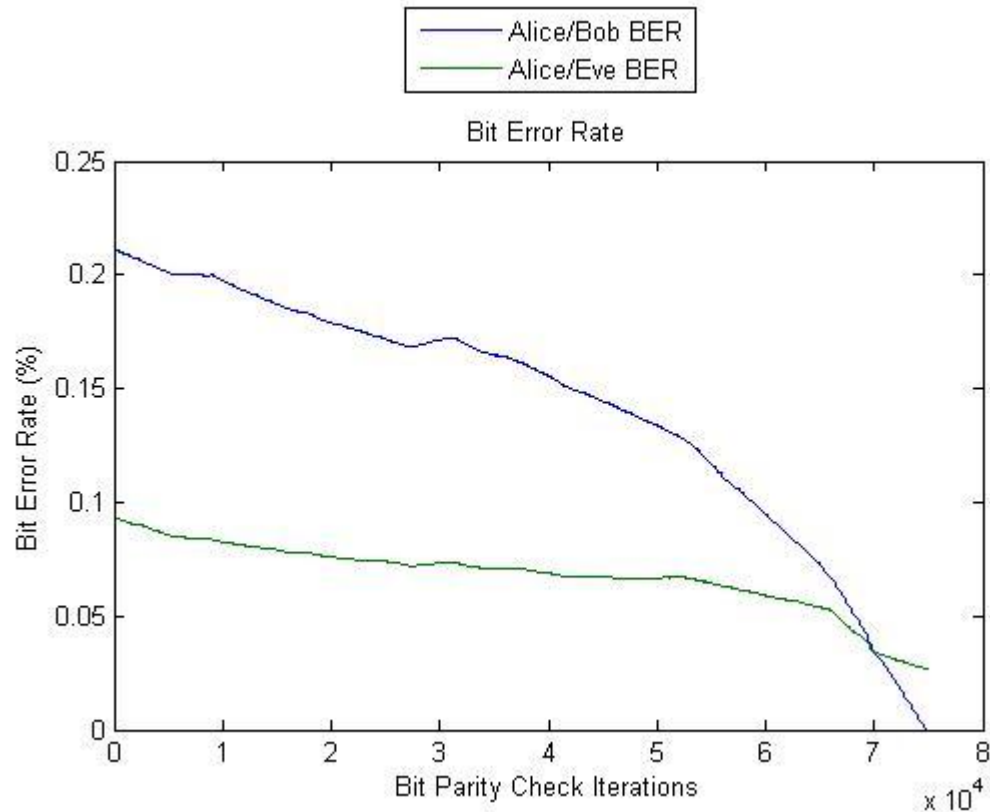
Source: [https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/Timing Based Encryption: Test Case 5](https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/Timing_Based_Encryption:_Test_Case_5)





# Timing based encryption

- Higher BER for Alice/Bob
- Long time in iterations
- Similar percentage in BER for Alice/Bob and Alice/Eve



Source:

[https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Eve\\_Output.jpg](https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Eve_Output.jpg)

# Our aims

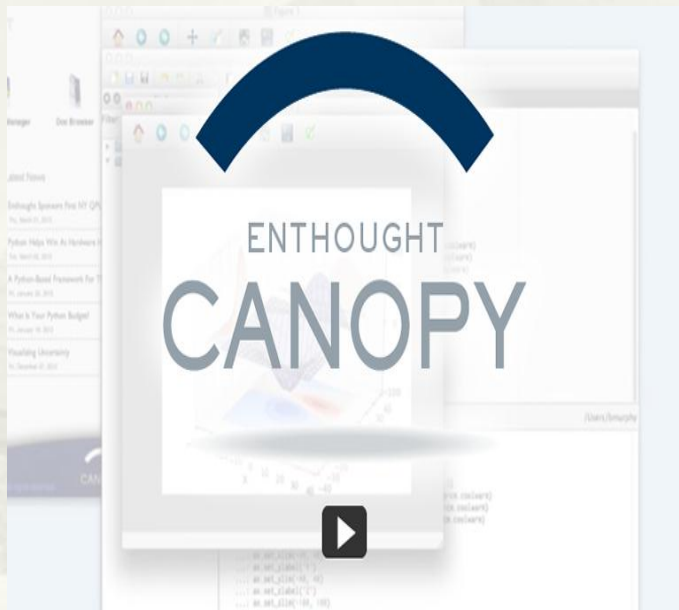
---

- \* The efficiency
- \* The reliability
- \* The speed
- \* The utilisation

# Approaches

## Software

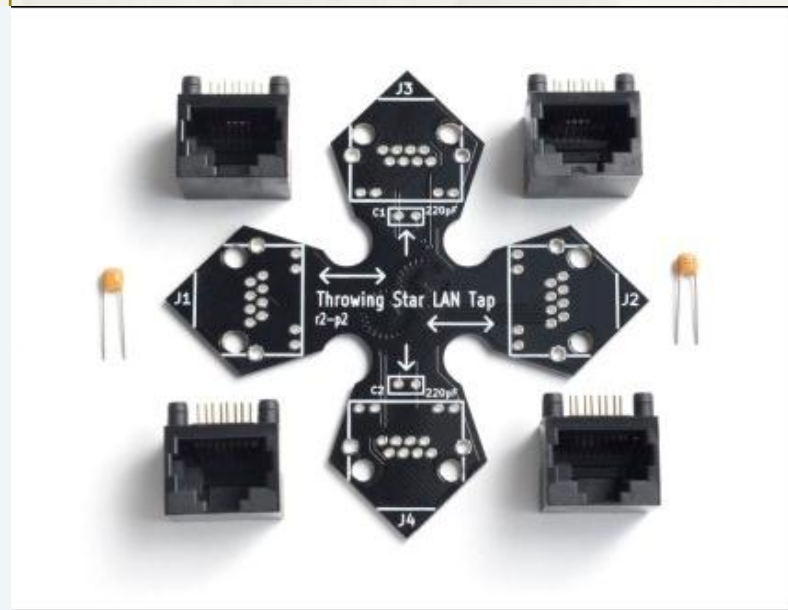
Own Personal Computer



Source:  
<https://www.enthought.com/products/canopy/>

## Hardware

Great Scott Gadgets



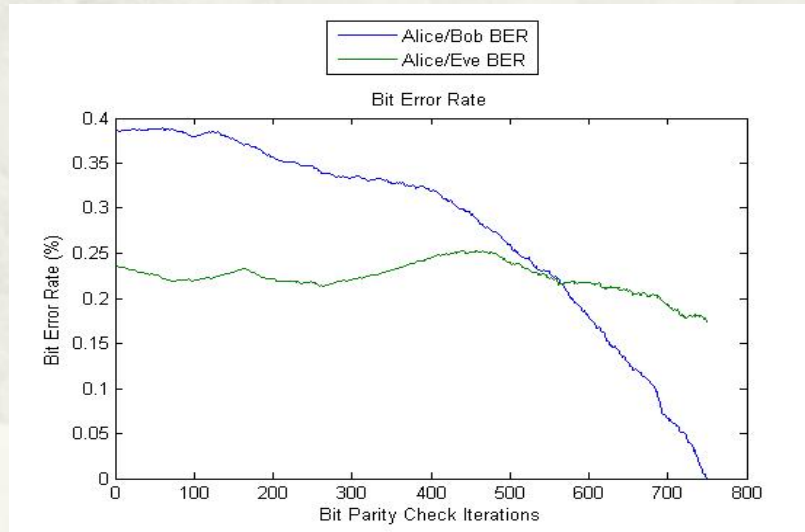
Source:  
<https://greatscottgadgets.com/throwingstar/>

# Approaches

## Software improvements of encryption

```
Channel BER confidence interval: <1.20e-01,3.52e-01>
Information reconciliation iterations: 4
Block size for privacy amplification: 4
Channel BER confidence interval: <1.03e-01,2.30e-01>
Information reconciliation iterations: 3
Block size for privacy amplification: 4
1111011010001000011110110111000000110010010101101010100011010010111101001001111
1111011101011010011000001011000001110110100000111100000010111010101000010010111
0100001111111010010111101001000000001011
```

Source: [https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Program\\_output.png](https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Program_output.png)

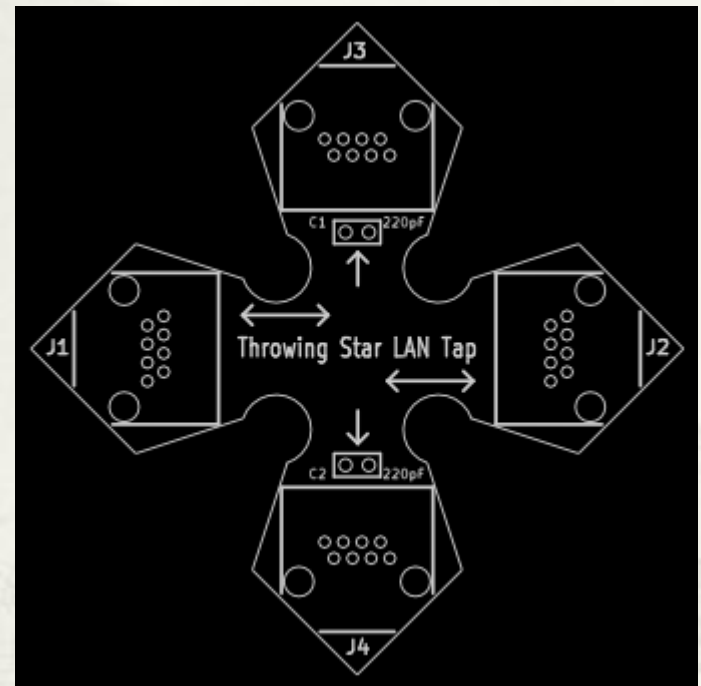


Source: [https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Eve\\_Output\\_Test21.jpg](https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Eve_Output_Test21.jpg)

# Approaches

## Network Tap (eavesdropper)

- J1, J2 – target network to be monitored
- J3, J4 – monitoring ports
- C1, C2 – forcing target network can be monitored



Source:

<https://greatscottgadgets.com/throwingstar/>

[2] Throwing Star LAN Tap, <https://greatscottgadgets.com/throwingstar/>

# Approaches

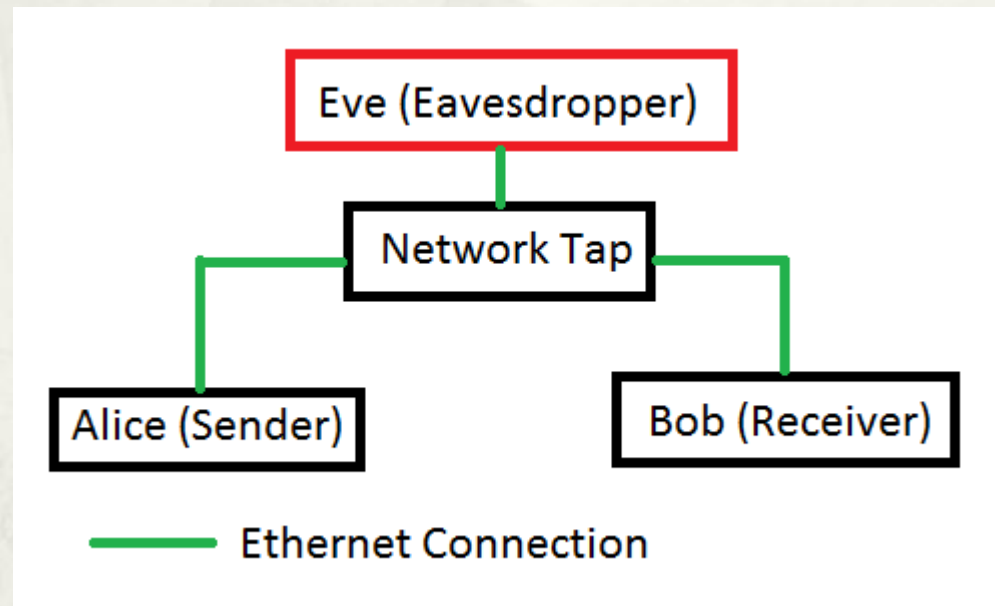
## Sender/Receiver

- Sender – Beagle board / PC
- Receiver – Beagle board / PC
- Eavesdropper – Beagle board



Source:

<http://beagleboard.org/Products/BeagleBone>

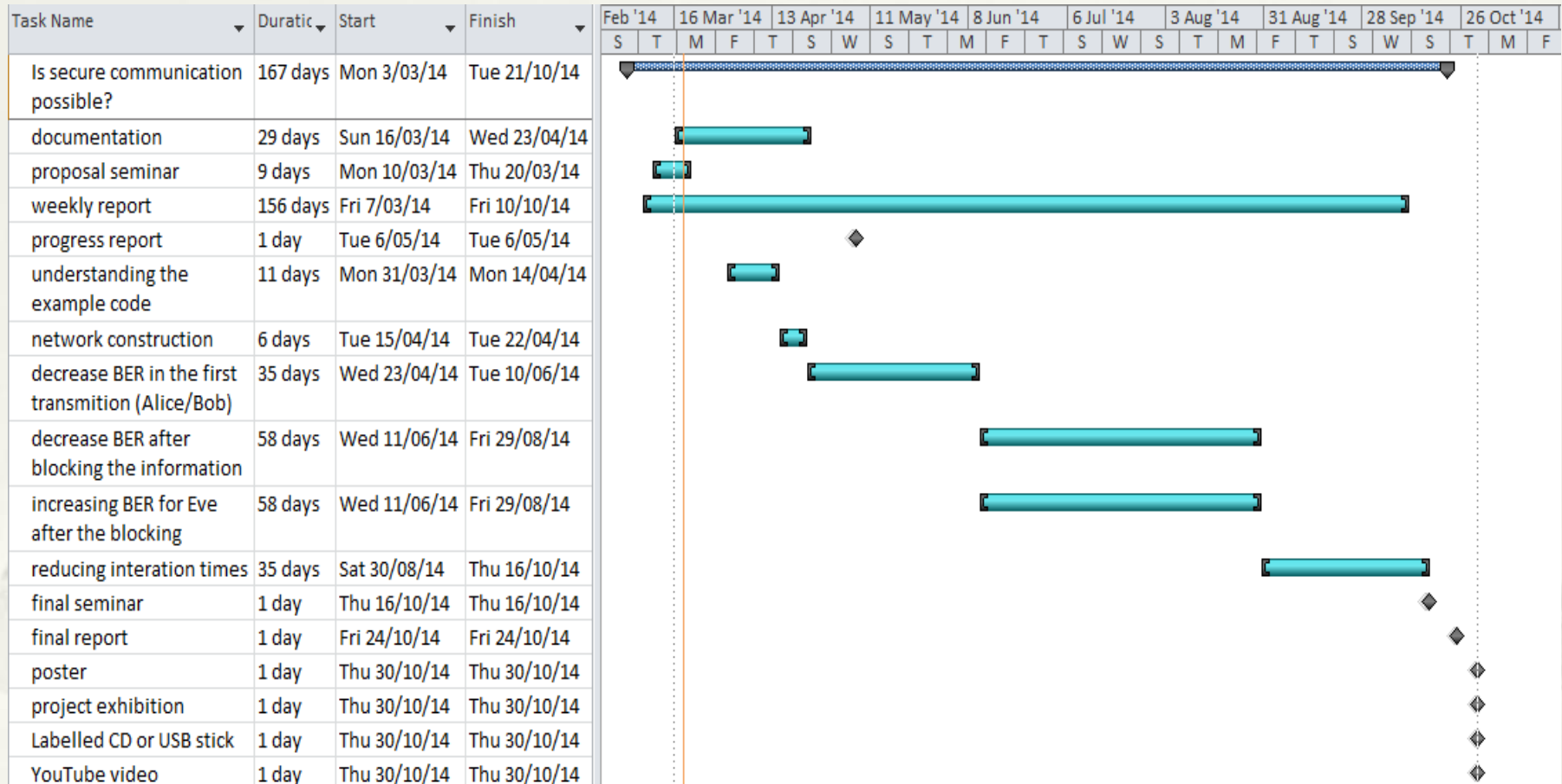


# Risk management

Risks	Posibility	Severity	Approaches
Unavailability of team member	Low	High	<ul style="list-style-type: none"> <li>Each member sign their own works but with help with each other</li> <li>Sharing the phone number and email</li> </ul>
SVN Blackout	Low	Low	<ul style="list-style-type: none"> <li>Sharing the document in Google Drive, file exchange or wiki to make sure each member and supervisors can share the working copies</li> </ul>
Lack of technical knowledge	High	High	<ul style="list-style-type: none"> <li>Keep talking with each other and supervisors to make sure we understand the technical aspects</li> <li>Finding useful information in youtube</li> </ul>
Physical parts do not arrive and/or do not work in time for project completion	High	Medium	<ul style="list-style-type: none"> <li>Ensure constant communication is sought with the suppliers regarding the progress of the delivery</li> <li>Expedite work on improvements to Timing Based Encryption</li> </ul>
Falling behind the schedule	medium	medium	<ul style="list-style-type: none"> <li>Re-evaluate the expectations</li> <li>Talking with supervisors to for extra times</li> </ul>
No final solution	Very high	Very low	<ul style="list-style-type: none"> <li>Ensure all progress have been completely documented</li> </ul>



# Time management



# Question and references

---

[1] L. Gunn, J. Chappell, A. Allison & D. Abbott, 'Physical-layer encryption on the public internet: a stochastic approach to the Kish-Sethuraman cipher'(June 2013)

[2] Throwing Star LAN Tap, <https://greatscottgadgets.com/throwingstar/>

[3] Derek Abbott's Wiki Project, 'Secure communications without key exchange', [https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/Main\\_Page](https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/Main_Page)