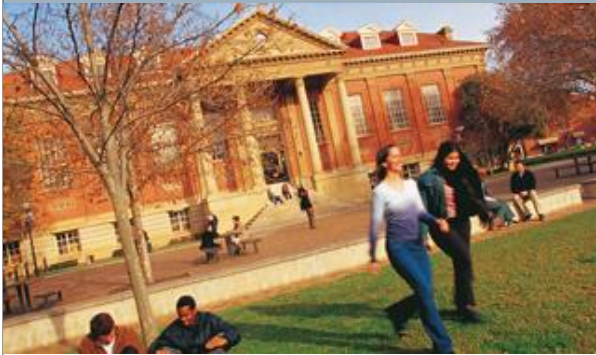




Is secure communications possible?



Yuanhao Liu, Christopher Lau

Supervisors:

Derek Abbott, Lachlan Gunn, James
Chappell



Outline

- **Introduction**
 - Is communication secure?
 - Power of eavesdroppers
 - Importance of cryptography
- **Encryption**
 - One Time Pad
 - Round Trip Times
- **Our Aims**
 - Efficiency
 - Reliability
 - Utilisation
- **Approaches**
- **Project Management**
- **Questions and References**



Introduction

Can communication be secure?



Sources: <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 eavesdropping

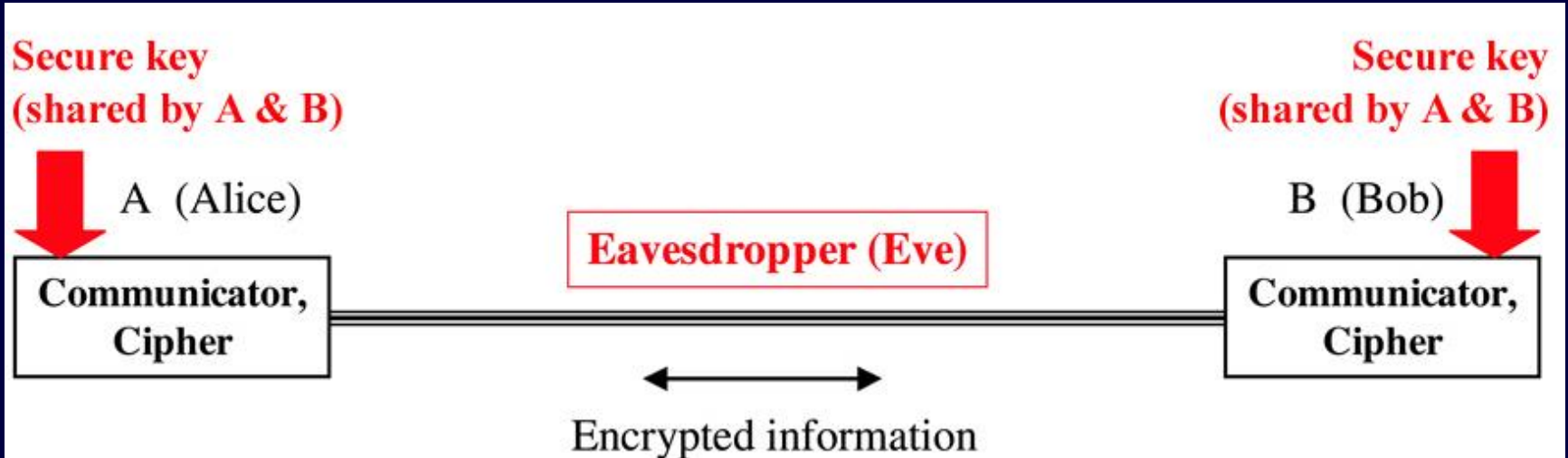


Sources: <http://blog.zap2it.com/pop2it/2013/06/nsa-leaker-edward-snowden-seeks-asylum-in-ecuador-lands-in-moscow-for-the-time-being.html> <http://rt.com/usa/obama-internet-wiretap-surveillance-009/>



Encryption

One-time pad – share the key



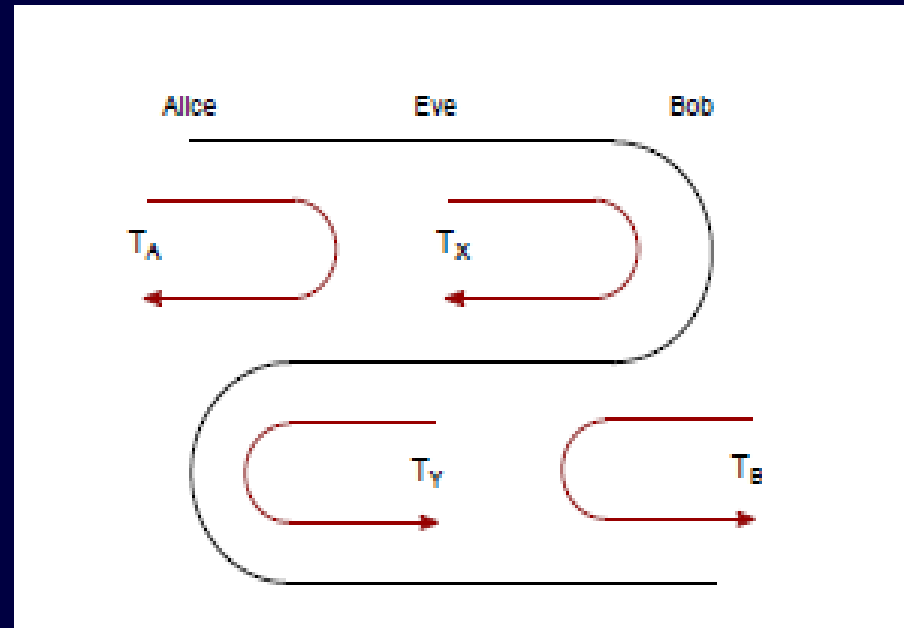
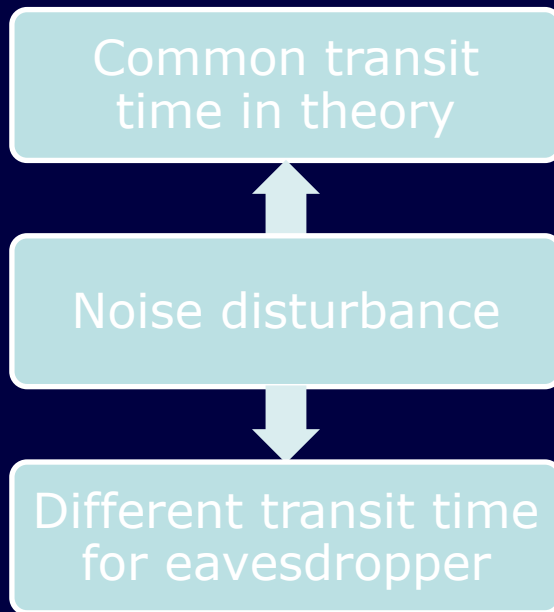
Source: <http://spie.org/x16669.xml>

The first unbreakable cipher [1]



Encryption

Round trip times



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



Timing Based Encryption

Noise channel

```

37 differences found. Use the toolbar buttons to navigate to them.
1 10010011111100010011010010100010111100101110101100100010001110100101 x 100100111111000010010100010100010111011011110001101110101100010001110100101 1
2 0110100100111001010100011001000000101100000000001100101000 01101001001110010101000011001000000101100000000011011110000000001100101000 2
3 111101010100100101100101011101001001100110000001110101010100100010 111101010010011001101011101000100110011000000110101010101001000100 3
4 0010000110010010001000100000001000100001000111111101011001110010001000 00100001100001100010000000100000001000000010000000011111101011001000100001000 4
5 110000101100111010010010101000010100101001011110000010100010010101 1000010110011101001010100001010010101001011110000010100010010101 5
6 1100100001111010100111010010111100000101000001000010101010010010100 11001000011110101001110100101111000001010000010000101010100100100100 6
7 101101000100010110101011101010111010101100101011001010101010100101 x 1011010001000100010110101011101010111010101101010110100100111001010101010101 7
8 11010100100100000011110101011111110101010101010101010101010101010101 x 1101010010000000000000000000000000000000000000000000000000000000000000000000 8
9 111010111101010101010010011101011100001111010101010000100001000010 11101011110101010101010101010001111010111000011111001000010100010001100011 9
10 10001010111010010000001010101010100011100001001110000101001001010 10000101111010010000001010101010100101000110100001000111000010100101010 10
11 010000100001000100010111001000001000010000000011101000001100 x 01000010000100010001011100100000100001000000011010000001100 11
12 1100001101010000110101100111001111010100001001010110100010000101110100 110001110101000011010111001110011101010000100101011010001000101110100 12
13 00110000100000000111010101010101010101010101010101010101010101010101 x 00110000100100000000000000000000000000000000000000000000000000000000000000 13
14 0010111100001010001110000111001111000000000101110001001010001100111010 0010111100001010001100000110001110000000001011100010010100011001110101 14
15 00100111001110111011100111010000100111010000100101010100001100100001100100 00100111001110111101110011101000010110100001001010100001100100001100100 15
16 11100100111111001111001000100000101001100111011011010100001010100010100 1110010011111100111100100010000001010011001111011011101000010101000101 16
17 01010011100010101100010000111000110000100010111000010110100001010001010 01010011100010101100010000111000010000100010110000101101000010100001010 17
18 011100000100010011101010000010101010100000000100001101010101010111011 x 01110000011000100001010100010111010111010100000000100001101010101000111011 18
19 0010101010111000001010001001010111111010010100010101010111000010000 x 00101010101110000010100010101011111101001010001000101010101010100010000 19
20 00100111000101001011010101010010000111000010100001000110110101010 x 0000010110000101001011101010101010010000011100001010000100001001110101010 20
21 1110100101010011010000000011001000001011100001010000101110100011001101 1110100101010011010100000000000000000000000000000000000000000000000000 21
22 10100111101010101010000001000011101111110101001011000100010000111101010 1000110101111010010101010000001000011101011111010101001100100110000111101010 22
23 0000101010111001000110001100011101011010110001100101000100001000010101 00001010111100100011010011000110101101010001100101000110000100001000010000 23
24 differences found. Use the toolbar buttons to navigate to them.
26 0101001000010100001110011111001010110000000110111010010100001000110011111 01010010000101000011100111001010101010000000110111010010000100001000110111 26
27 011010100010011111001000010111000100101100010001001010000110011110101000 011010100001001111100100001011100011000100100100000001010100001001110101000 27
28 01101000101001111010000001001010100100001110010111100100001111111100 011101000010001111010000001001010100100010011100101111001000011111111100 28
29 0010101111000001000010000100001000010000100001000010000100001000010000 x 00101011110000010000100001000010000100001000010000100001000010000100001000 29
30 1000010100010001000010000100001000010000100001000010000100001000010000 x 100001010001000010000100001000010000100001000010000100001000010000100001000 30
31 100000000101000010010011011000101000101011010000100001011100101000011 1000000001010000101000010100001010000100001011100101000011 31
32 1000001111101010101000101111010100010100110011101010010000000110101 100000111110101010100010110011001100001001110011001001110101000000011010 32
33 0100001111100000000101010000111000010100110101101010101010100010001 x 010000111110000000010101010000111001000011001000010001101011010101010100010001 33
34 1101011100110101000001000010101010101000001110000010101011101110 11010111001101010100000100001010101010100000111000001010101000001110000010101110 34
35 11101001011110100000111000010100000111010111001100001000000101010000100 11010010101111010000011100001010000011010111001100001000000010100000100 35
36 00010100011101111000110000100100011101011110100001001000000000101001001 0001010001110111100011000010010001110101111010000100100000000101001001 36
37 110110000001011000111000101011101010110000101010100000010010101010101 1101100000010110001110001010111010101100000010010101010101 37
38 100010100001111000000000101010101110100010111000101110000101110101001 x 1000101000011110000000001010101011101000101110000101110000101110000101110001001 38
39 0001011101011110001100111001000110100000011111111100010010101010001 0001011101011110001100110010001101000001011111111100010010010101010001 39
40 1101111000100011110100110000100001010101110011010111011000001110 1101111000100011110100110000100001010101100111010110101000001110 40
41 01110001000000100010010000101010100001000010100011101101101010000001100 x 011100010000100000010000001000010101010000100001010000111011010100000001100 41
42 0011000101010111000011100111110010101010100000110100000000110101000101 00110001010101011100001110011110010101010100001010010000000110101000101 42
43 0101000001110010101010100100010101010000111101111110000010101010101010 0101000001110010101010100100010101010000100010110000100000001111000001001010 43
44 11100001001000000001011000111110101011001010001101000000100001000100011 1110000100100000000101100011111010101100101000110100000010000100010001 44
45 0110010101010110101000100011000100011110111111100000101011011011 011001010101011010100010001100010001010100000111111110111000001010110111 45
46 11101011001000111001000100101110100001001010001110101100101010001001 111010110010001110010001001010001110101010001000101000110101100101000100 46
47 1001000110000101010101011101101000101010001011001000101110101001100 x 100100011000001010101010111011010001010100011001100001010100010101111001100 47
48 10110000011001100010100011101000001101110010101011100000101110000 1011000001100111001010001110100000101110000010111010101011100001001000111100 48
49 1100001100001010001001001010000001110000101001000100010000011001100001 1100001100001010001001001010000001110001001000100101000000011001100001 49
50 1100000101000001000010100101111001011010000100000000111011001110011 110000010100000100000101000101111001011010000100100001110110011001100 50
51 11011110100000101110010001110101000010010101000001011001101110100001 1101111010100000101110010001110101000010000010110011011010100001 51
52 111101010000001001001000000111010100001000100000110100011011100001000001 111101010000000100100000011101010000100001000010100001011100000100001 52
53 1010100000101000100001010101010011110111100000101001000111011010101111 10101000001010000100000101010101001110111100000101001000011101010101111 53

```

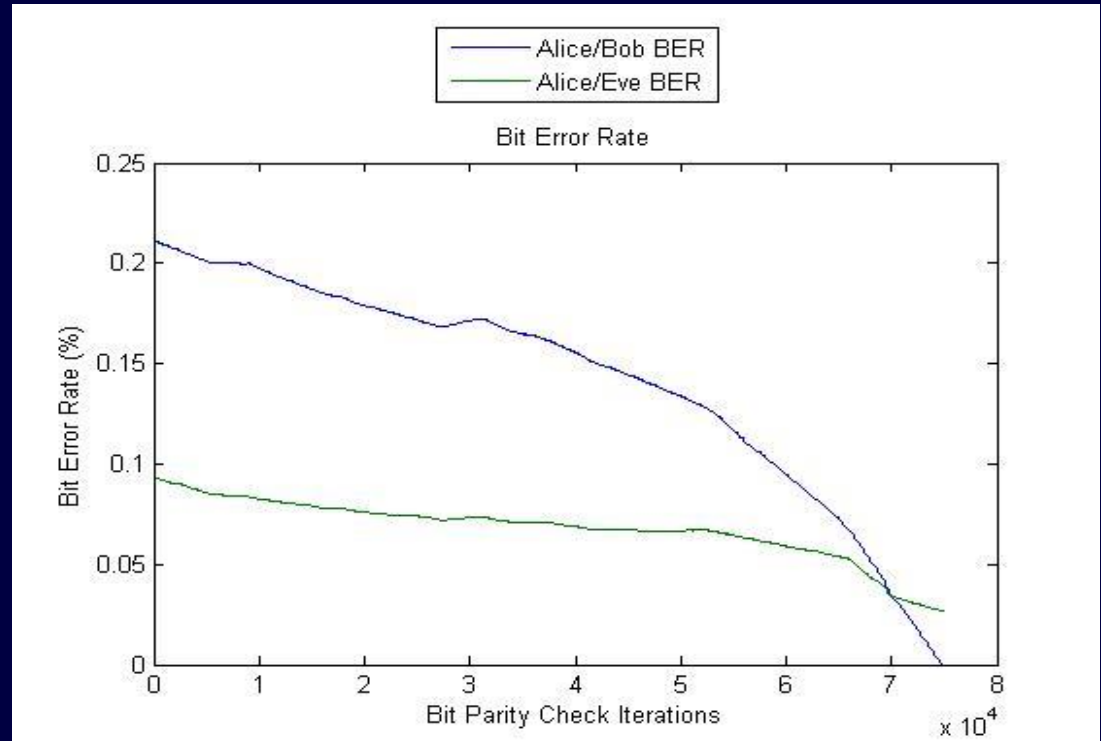
The length of the two bit streams is 14324
The number of errors between the two bit streams is 195
The BER between Bob and Alice is 1.361%

Source: 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 iteration time
- 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



Our aims

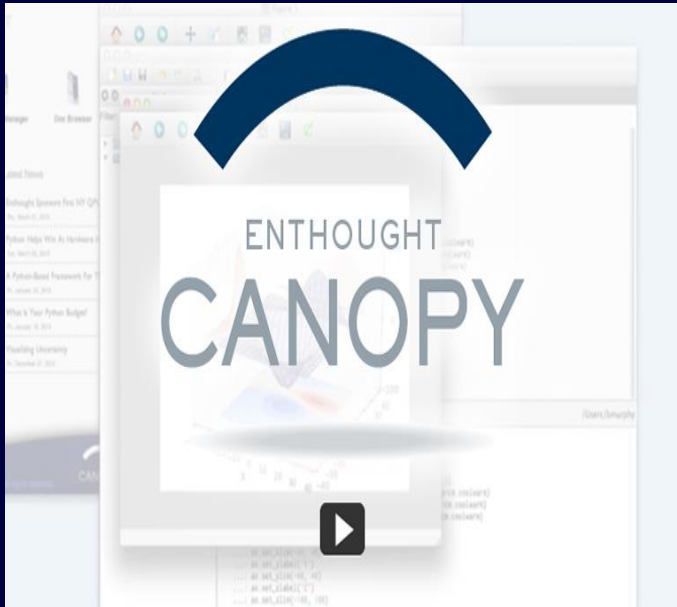
- Efficiency
- Reliability
- Utilisation



Approaches

Software

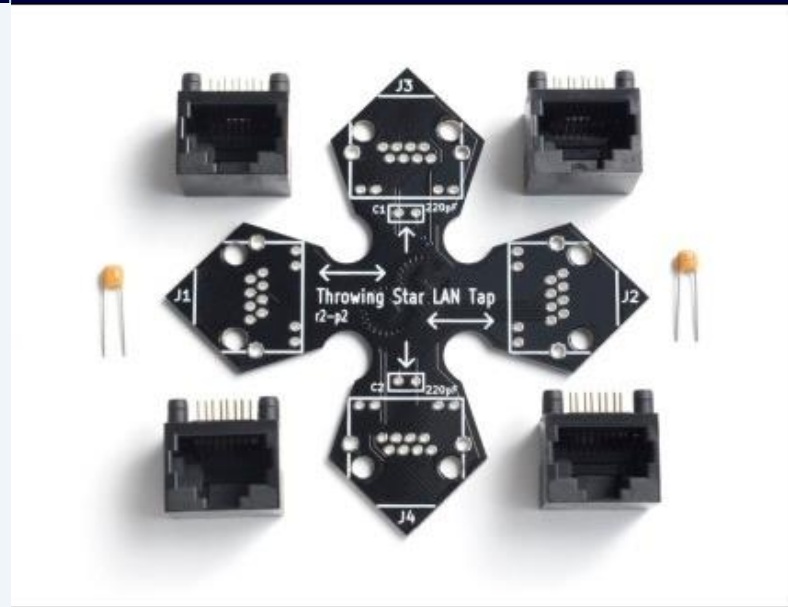
Own Personal Computer



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

Hardware

Great Scott Gadgets



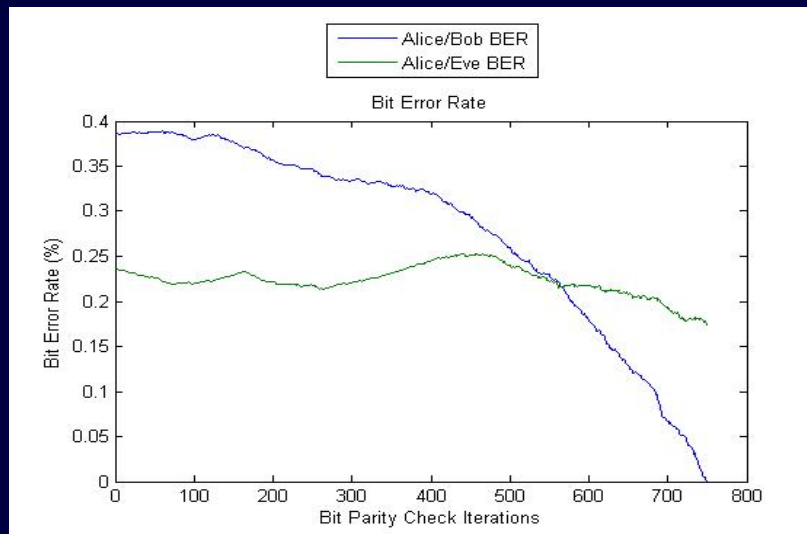
Source:
<https://greatscottgadgets.com/throwingstar/>



Approaches

```
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
11110110100010000111101101110000001100100101011101010100011010010111101001001111
1111011101011010011000001011000001110110100000111100000010111010101000010010111
01000011111111010010111101001000000001011
```

Source: https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Program_output.png



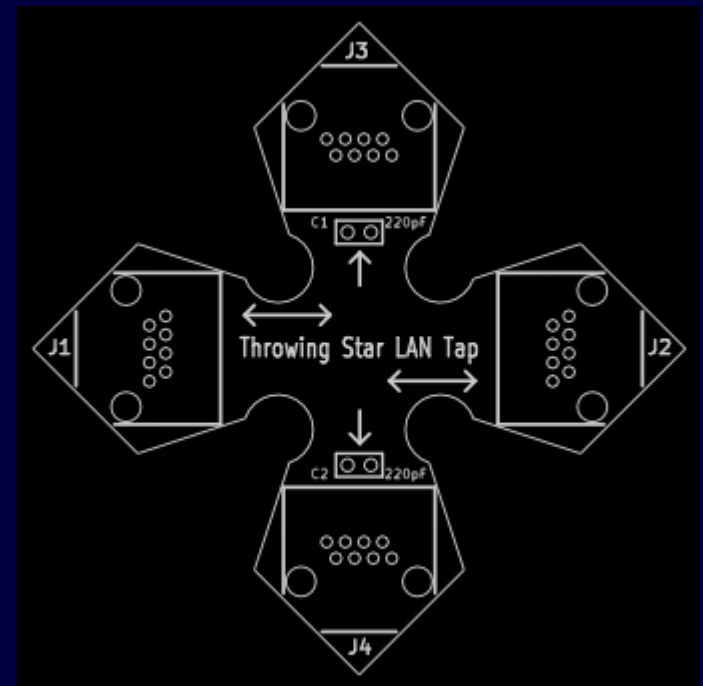
Source: https://www.eleceng.adelaide.edu.au/personal/dabbott/wiki/index.php/File:Eve_Output_Test21.jpg



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>



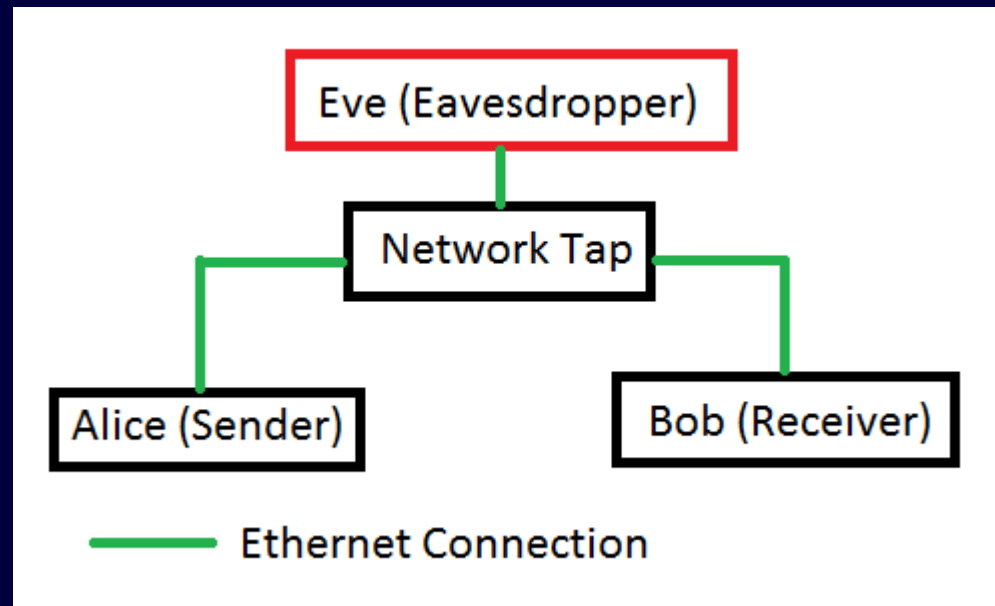
Approaches

Sender/Receiver

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



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



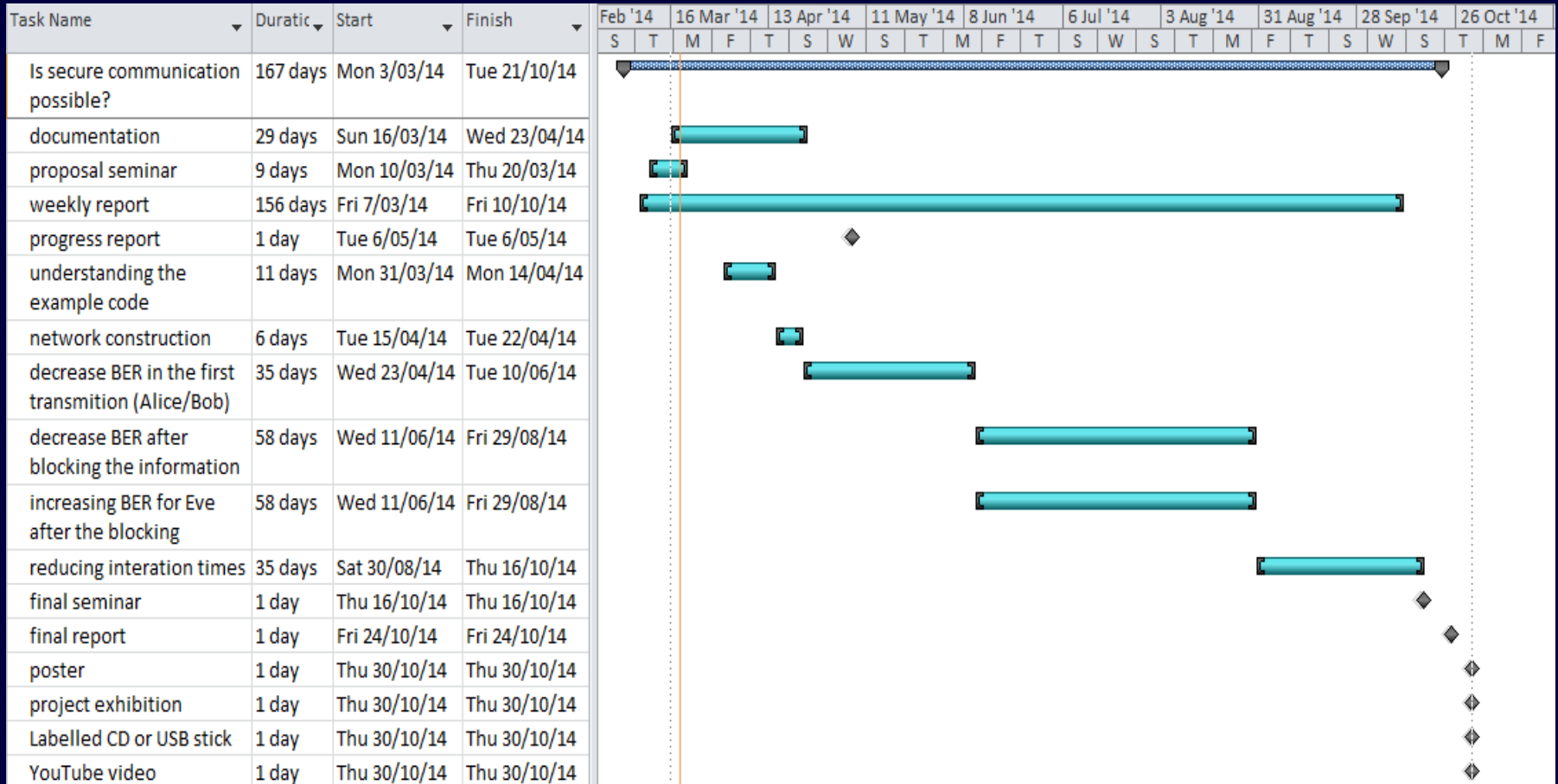


Risk Management

Risk	Likelihood	Severity	Avoidance / Mitigation Strategies
Project files missing or are not accessible	Very Low	Low	We will ensure that all work related to the project is stored on the cloud via the project's Wiki, Google Drive and Dropbox and is accessible by both team members.
Unavailability of team member	Low	Medium	Team members will keep each other informed about their work on the project which will allow their work to continue should a team member be unavailable.
Physical parts do not arrive and/or do not work in time for project completion	High	Medium	Ensure constant communication is sought with the suppliers regarding the progress of the delivery in order to plan for contingencies which include expediting work on improvements to Timing Based Encryption
Falling behind schedule due to increased complexity of work undertaken	Medium	Medium	Reevaluate the scope of the project and if necessary restrict the scope to focus, among other things, on improving the functionality of the Timing Based Encryption and the encryption's efficiency.
Not finding a solution to our project	Very High	Very Low	Ensure any progress made is documented and can be used as the basis for the final seminar and exhibition



Time Management





Questions 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