School of Electrical & Electronic Engineering

THE UNIVERSITY of ADELAIDE

Secure Communication
without Key Exchange

Honours Project 2013
Aleks Kojic
Michael Parisotto

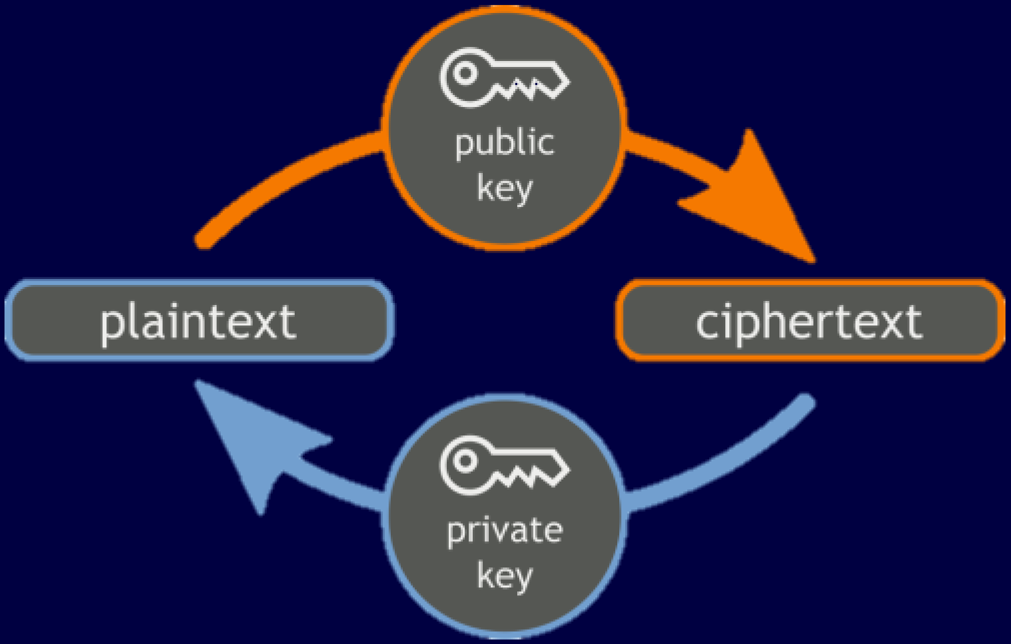
Supervisors:
Derek Abbott,
James Chappell & Lachlan Gunn

Seminar Overview

- Objectives & Context
- Project Significance & Implications
- One-Time Pad in the KS Cipher
- Geometric Algebra 3D & 4D
  - Introduction
  - Analytical Work & C++ Program
  - CLUViz Demonstration
  - Summary
- Timing-Based Physical Layer Encryption
- Project Management
- Conclusion
- Question Time & Key References

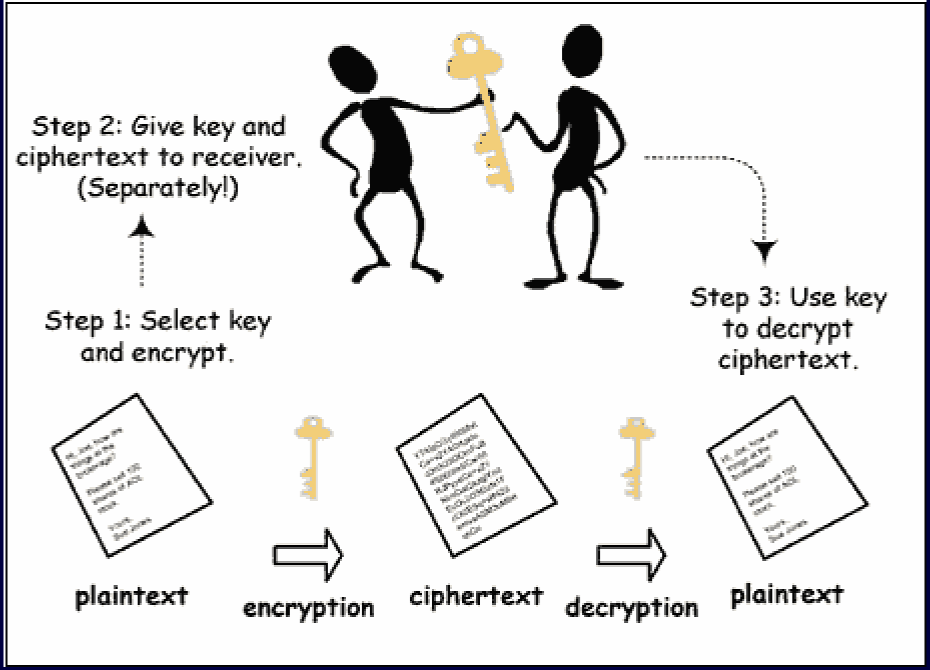
Introduction

Public Key Cryptography



Introduction

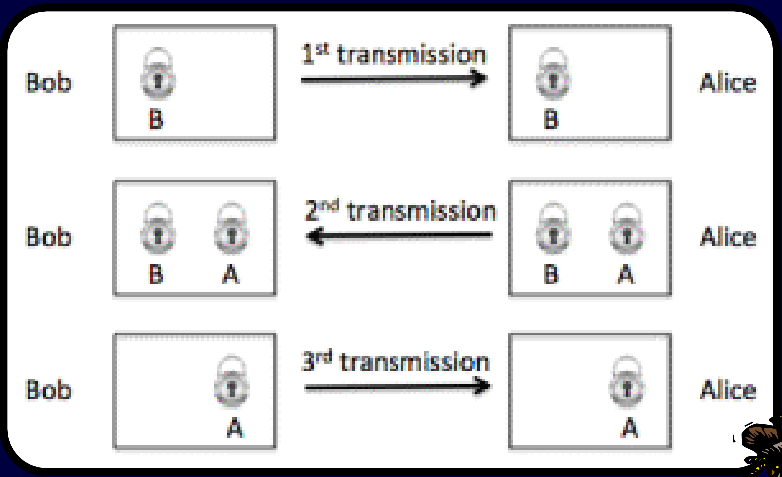
Symmetric Key Systems


Step 2: Give key and ciphertext to receiver. (Separately!)
Step 1: Select key and encrypt.
Step 3: Use key to decrypt ciphertext.
plaintext
encryption
ciphertext
decryption
plaintext

The Double-Padlock Protocol

Kish-Sethuraman (KS) Cipher - The Double Padlock Protocol

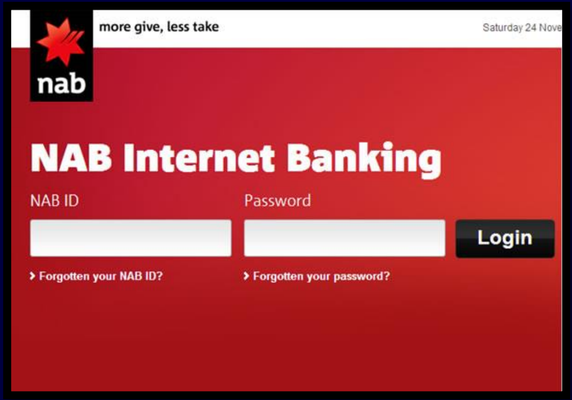
What it would mean?



Laszlo Bela Kish
Professor, Texas A&M University

Image: J. Chappell and D. Abbott, The Double –Padlock Problem, http://scholar.google.com.au/citations?user=fVJ8twEAAAAJ&hl=en

Project Significance & Implications


more give, less take

Saturday 24 Nove

nab

NAB Internet Banking

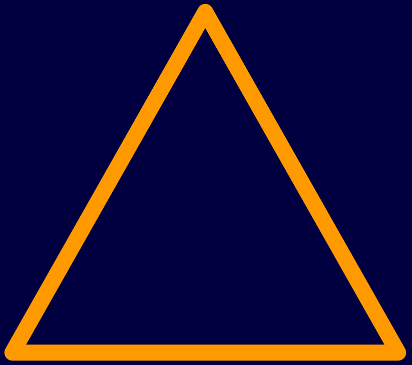
NAB ID

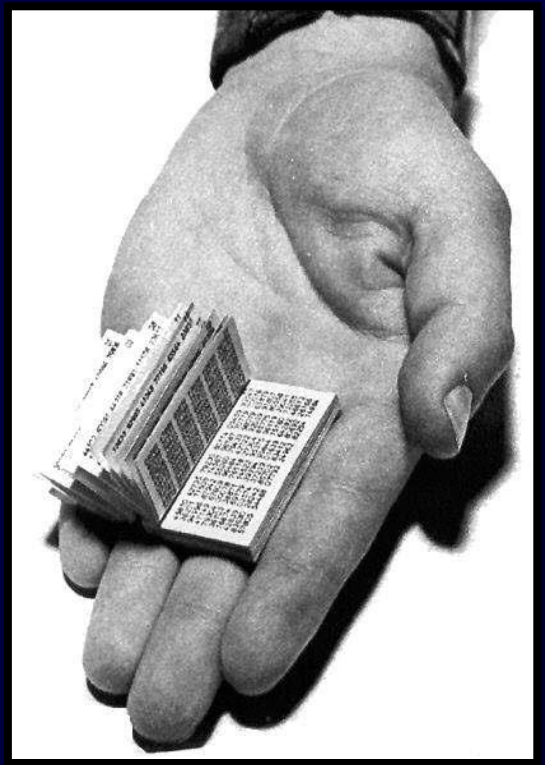
Password

Images: aerospace.firetench.com, http://www.nab.com.au, http://www.jyi.org/wp-content/uploads//GPS_Satellite_NASA_art-iif.jpg

The One-Time Pad

Key Elements of the OTP





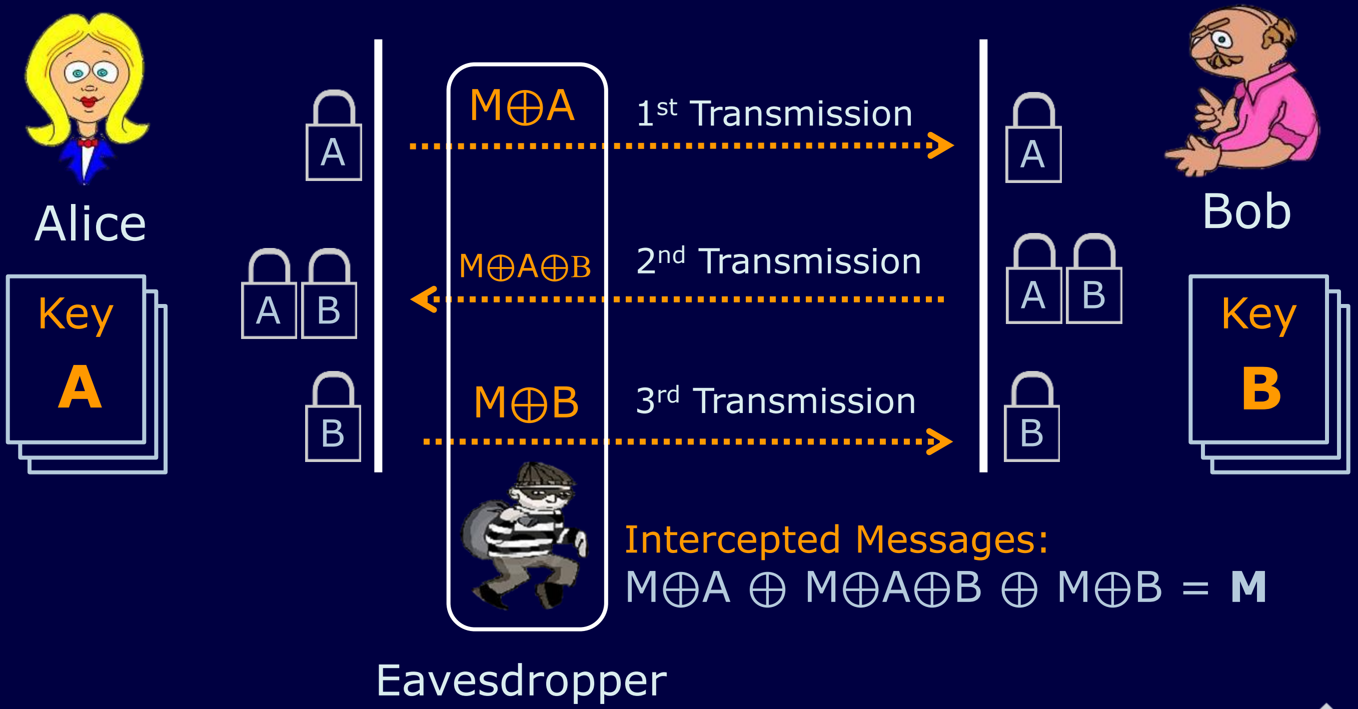
Small Russian One-Time Pad captured by MI-5

Image: www.ranum.com/security/computer_security/papers/otp-faq/

Using a One Time Pad in the KS-cipher

What if Alice & Bob each had their own unique OTP?

The initial Message is M



Alice

Key A

Bob

Key B

$M \oplus A$ 1st Transmission

$M \oplus A \oplus B$ 2nd Transmission

$M \oplus B$ 3rd Transmission

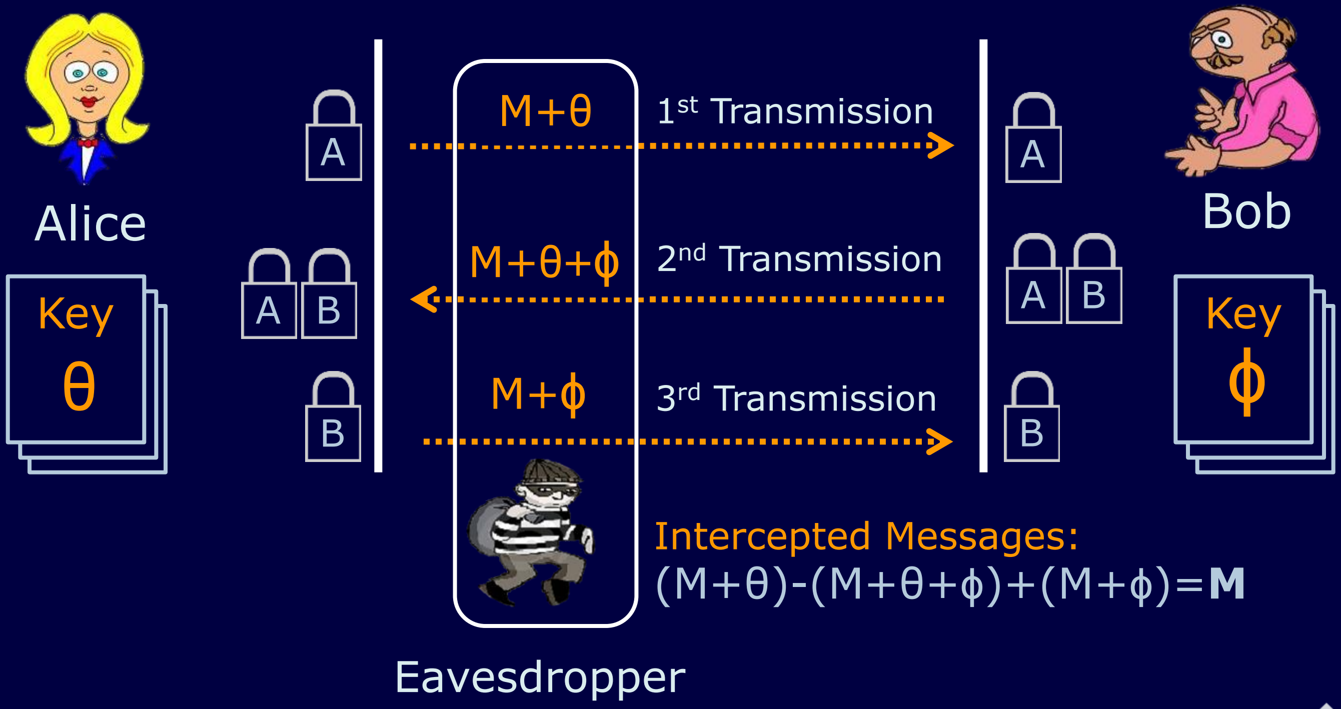
Intercepted Messages:

$M \oplus A \oplus M \oplus A \oplus B \oplus M \oplus B = \mathbf{M}$

Eavesdropper

Using a One Time Pad in the KS-cipher

The XOR approach can be generalised to rotations in 2D



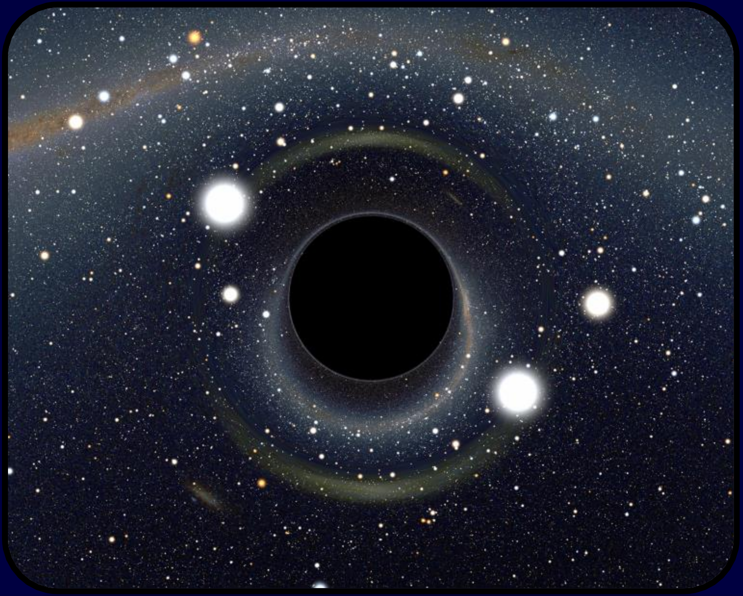
Intercepted Messages:

(M+θ)-(M+θ+ϕ)+(M+ϕ)=**M**

Geometric Algebra

A Powerful Mathematical Tool

Ability to easily handle rotations in N-dimensions



$$v' = e^{\frac{ir\theta}{2}} . v . e^{\frac{-ir\theta}{2}}$$

De Moivre's theorem applies

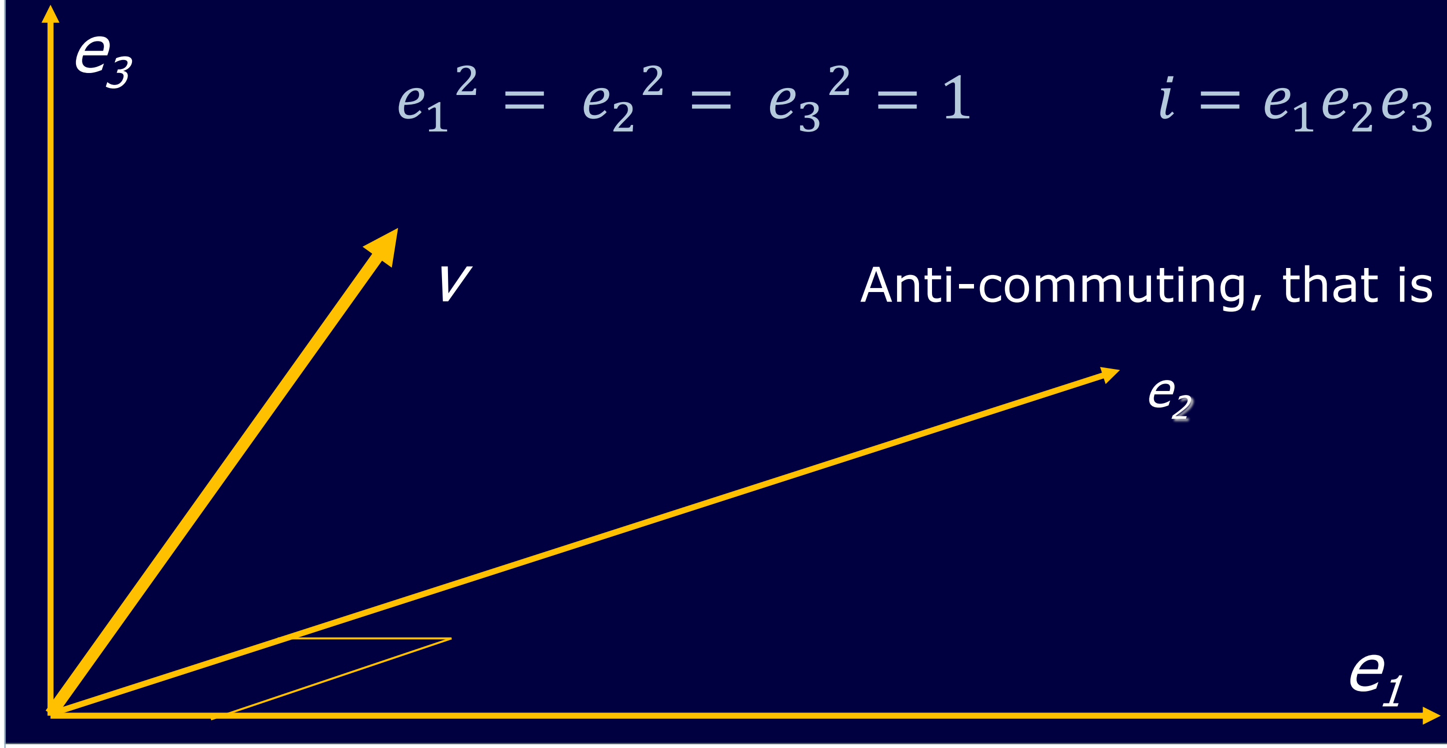
Image: apod.nasa.gov

Geometric Algebra

Vector v is defined as $\boldsymbol{v} = a_1 e_1 + a_2 e_2 + a_3 e_3$

$$e_1{}^2 = e_2{}^2 = e_3{}^2 = 1 \qquad i = e_1 e_2 e_3$$

Anti-commuting, that is $e_1 e_2 = -e_2 e_1$

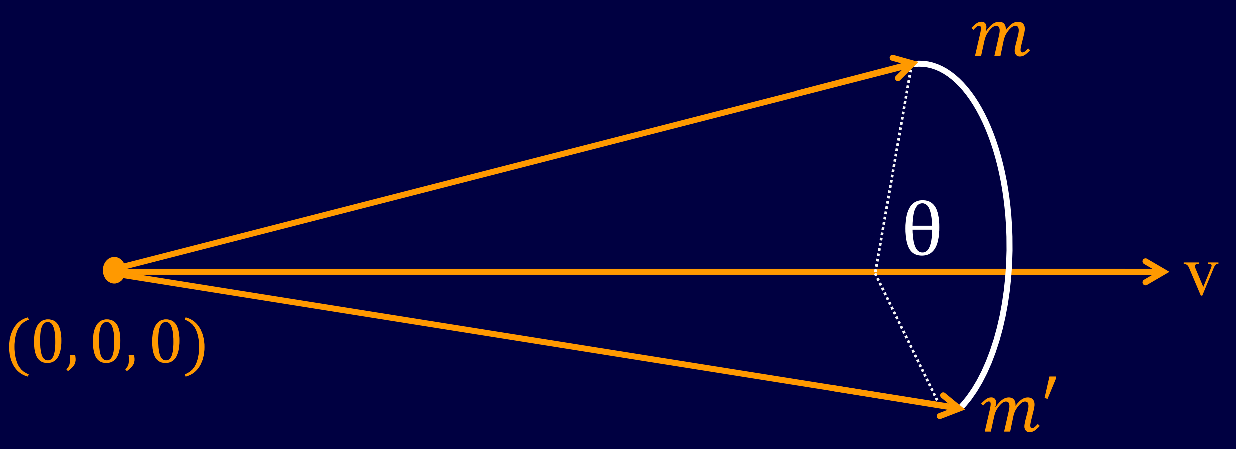


Geometric Algebra

Initial Message Vector $\boldsymbol{m} = m_1 e_1 + m_2 e_2 + m_3 e_3$

$$R = e^{iv\theta/2}$$

$$\therefore \boldsymbol{m}' = e^{iv\emptyset/2}.\boldsymbol{m}.e^{-iv\emptyset/2}$$



Geometric Algebra

Rotation Operators of Alice & Bob

$$R_A = e^{iv\theta/2} \qquad R_B = e^{iw\emptyset/2}$$

$$\boldsymbol{m}_{final} = \widetilde{R_B}\widetilde{R_A}R_B R_A\ \boldsymbol{m}_{initial}\ \widetilde{R_A}\widetilde{R_B}R_A R_B$$

$$R_A R_B - R_B R_A = -\sin\frac{\emptyset}{2}\sin\frac{\theta}{2}\ v \times w \ \boxed{= 0}$$

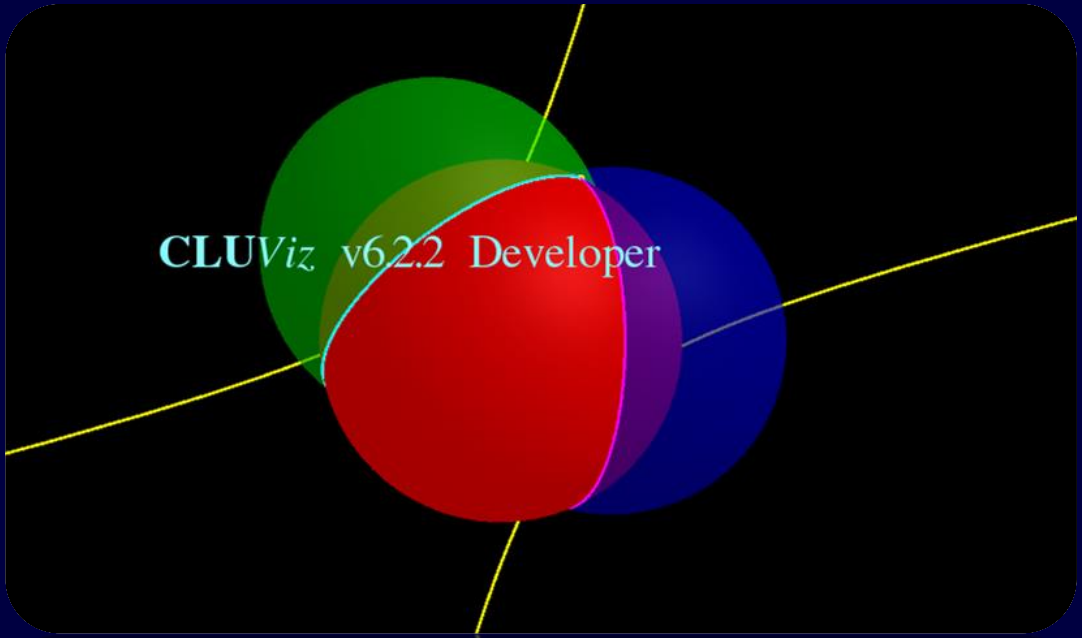
Geometric Algebra

- C++ Program
- 4D Analytical Work
- Still wanted to explore and visualize 4D Rotations

Source: James Chappell

CLUViz Demonstration

- 3D CLUViz Program
- Proof of requirement for parallel rotation axes
- Complexity of 4D Rotations



Geometric Algebra Summary

Information Theory revealed a hole in our approach

Shannon's work on the capacity of a *Binary Symmetric Channel*

Secrecy Rate → C_s

Alice's Information → X

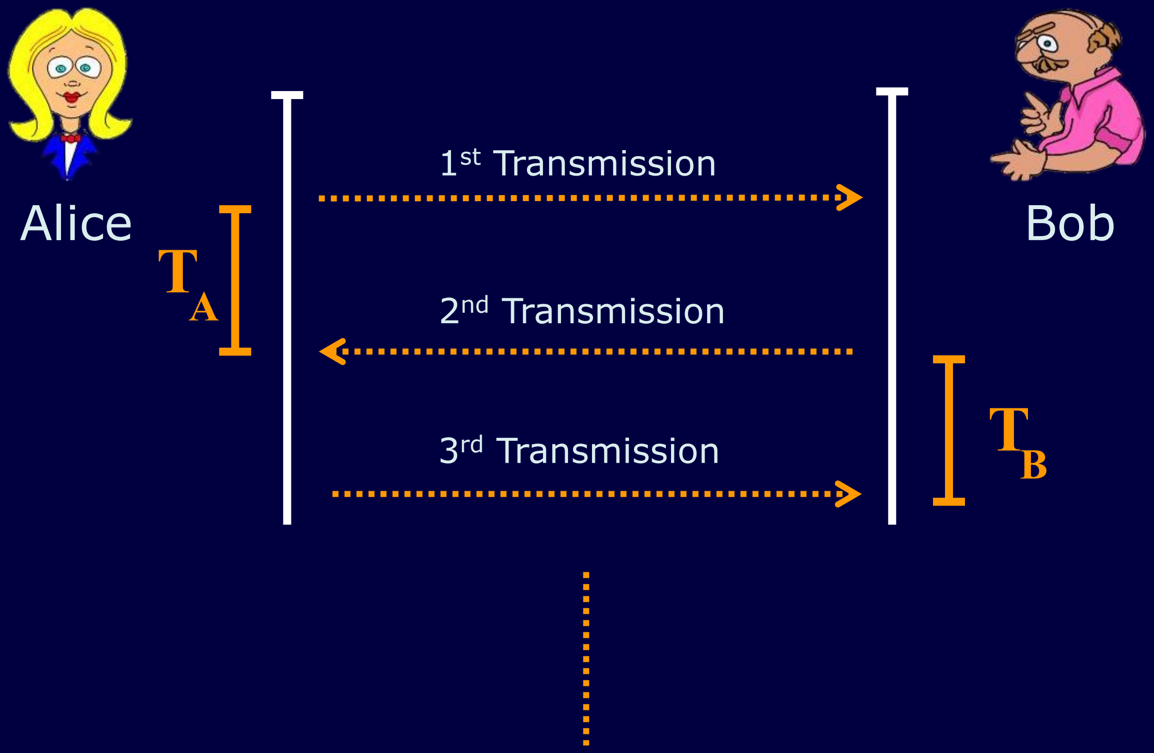
Bob's Information → Y

$$C_s \leq I(X,Y)$$

Found a new approach in Timing-based Physical Layer Encryption

Timing-Based Physical Layer Encryption

What is it? How can it be used?



Alice

Bob

1st Transmission

2nd Transmission

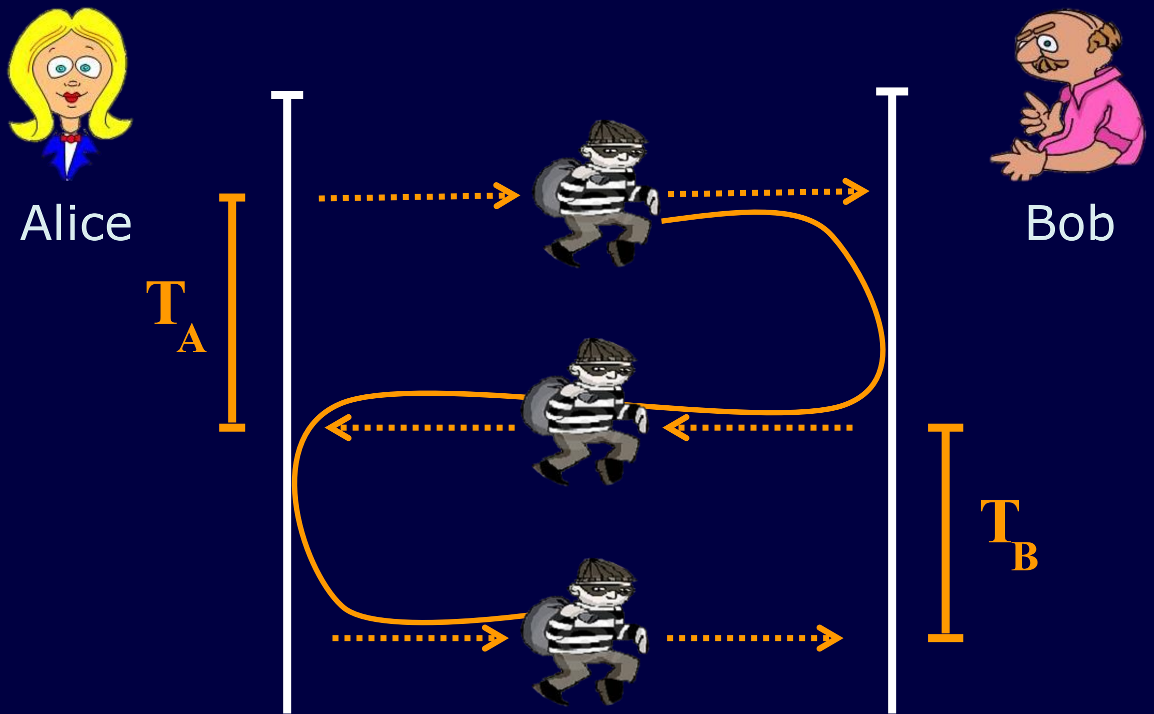
3rd Transmission

T_A

T_B

Timing-Based Physical Layer Encryption

Practical Setup



Timing-Based Physical Layer Encryption

Bit Stream Generation

$$\begin{pmatrix}0.363\\0.407\\0.356\\0.333\\0.565\\0.345\end{pmatrix} \rightarrow 110010....$$

$$rtt(i) > median \rightarrow 1$$

$$rtt(i) < median \rightarrow 0$$

Timing-Based Physical Layer Encryption

Bit Parity Checks

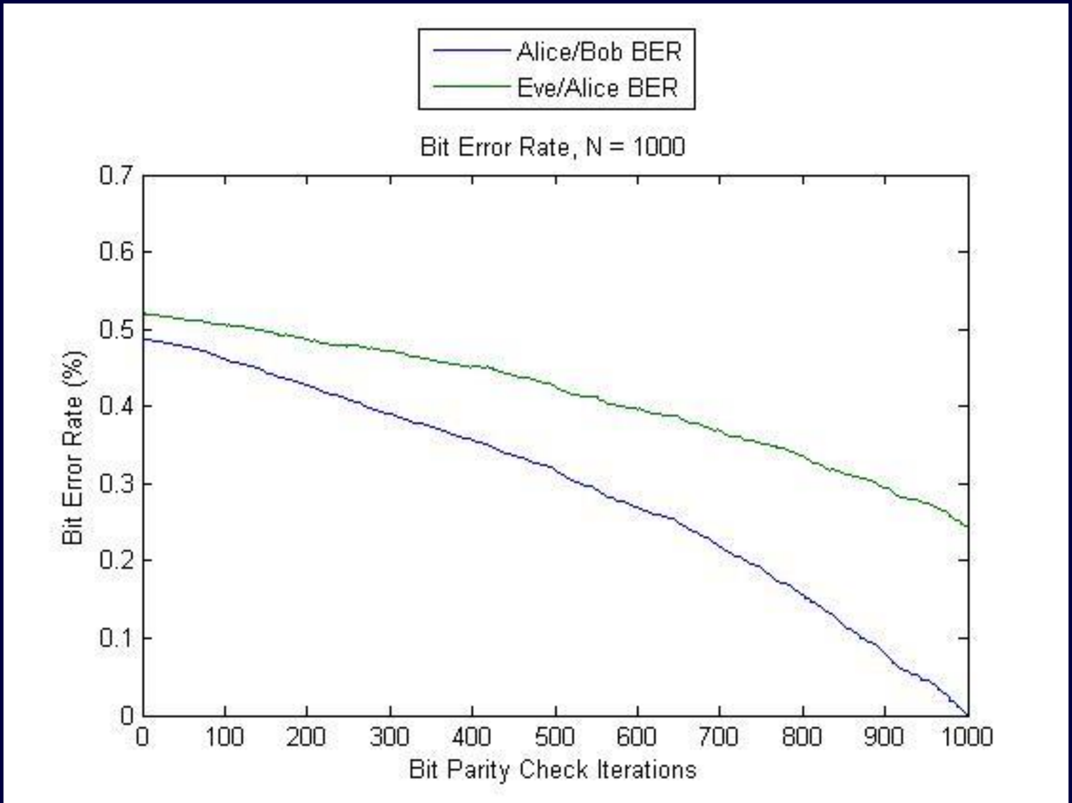
$$Alice \quad 10\ 01\ 11\ 01 \rightarrow 1\ 0\ 1$$

$$Bob \quad 11\ 01\ 10\ 10 \rightarrow 1\ 0\ 1$$

$$Eve \quad 01\ 01\ 00\ 11 \rightarrow 0\ 0\ 0$$

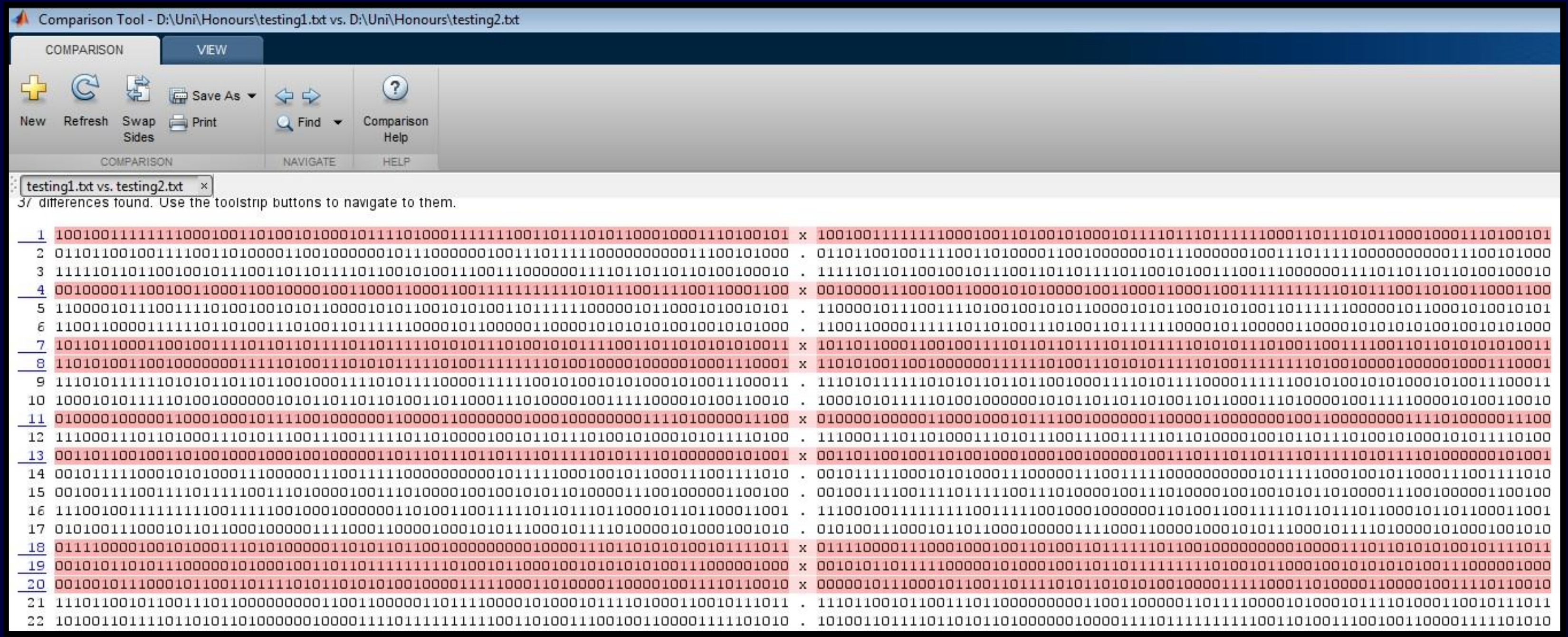
Timing-Based Physical Layer Encryption

Bit Parity Checks

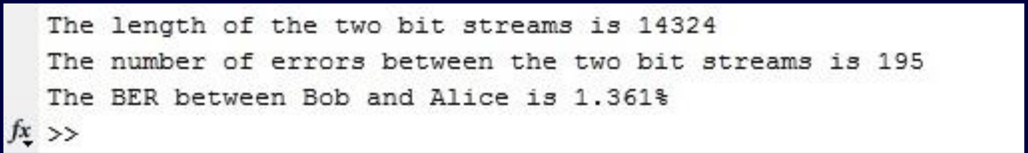


Timing-Based Physical Layer Encryption

Matlab Analysis of Output


Comparison Tool - D:\Uni\Honours\testing1.txt vs. D:\Uni\Honours\testing2.txt
COMPARISON
VIEW
New
Refresh
Swap Sides
Save As
Print
Find
Comparison Help
COMPARISON
NAVIGATE
HELP
testing1.txt vs. testing2.txt

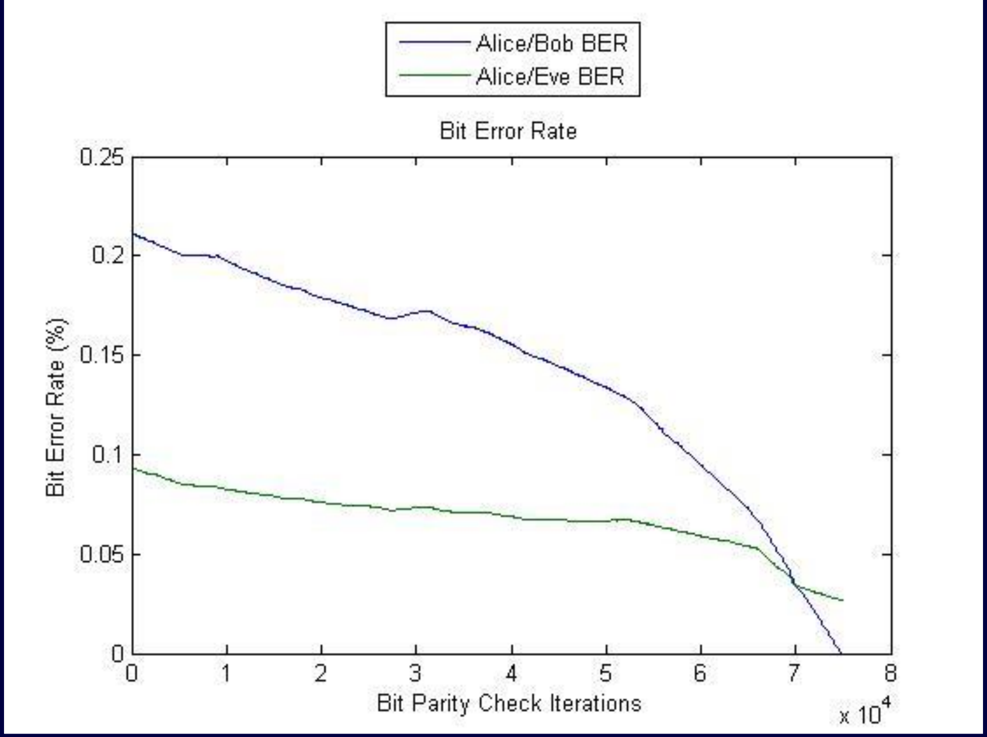
```
37 differences found. Use the toolstrip buttons to navigate to them.

 1 10010011111111000100110100101000101111010001111111001101110101100010001110100101 x 10010011111111000100110100101000101110111011111110001101110101100010001110100101
 2 0110110010011110011010000110010000001011100000001001110111110000000000011100101000 . 0110110010011110011010000110010000001011100000001001110111110000000000011100101000
 3 111110110110010010111001101101111011001010011100111000000011110110110110100100010 . 111110110110010010111001101101111011001010011100111000000011110110110110100100010
 4 001000001110010011000110010000100110001100011001111111111101011100111100110001100 x 001000001110010011000101010000100110001100011001111111111101011100110100110001100
 5 110000101110011110100100101011000010101100101010011011111110000010110001010010101 . 110000101110011110100100101011000010101100101010011011111110000010110001010010101
 6 11001100001111110110100111010011011111100001011000001100001010101010010010101000 . 11001100001111110110100111010011011111100001011000001100001010101010010010101000
 7 101101100011001001111011011011110110111101010111010010101111001101101010101010011 x 101101100011001001111011011011110110111101010111010011001111001101101010101010011
 8 1101010011001000000011111010011101010111110100111111111010010000100000010001110001 x 1101010011001000000011111010011101010111110100111111111010010000100000010001110001
 9 11101011111101010110110110010001111010111100001111110010100101010001010011100011 . 11101011111101010110110110010001111010111100001111110010100101010001010011100011
10 100010101111101001000000010101101101101001101100011101000010011111000010100110010 . 100010101111101001000000010101101101101001101100011101000010011111000010100110010
11 0100001000001100010001011110010000000110000110000000100010000000001111010000011100 x 0100001000001100010001011110010000000110000110000000100110000000001111010000011100
12 11100011101101000111010111001110011111011010000100101101110100101000101011110100 . 11100011101101000111010111001110011111011010000100101101110100101000101011110100
13 001101100100110100100010001001000001101110110111101111011111010111101000000101001 x 001101100100110100100010001001000001001110110111101111011111010111101000000101001
14 001011111000101010001110000001110011111000000000010111110001001011000111001111010 . 001011111000101010001110000001110011111000000000010111110001001011000111001111010
15 001001111001111011111100111010000100111010000100100101011010000111001000001100100 . 001001111001111011111100111010000100111010000100100101011010000111001000001100100
16 11100100111111111001111100100010000001101001100111110110111011000101101100011001 . 11100100111111111001111100100010000001101001100111110110111011000101101100011001
17 01010011100010110110001000001111000110000100010101110001011110100001010001001010 . 01010011100010110110001000001111000110000100010101110001011110100001010001001010
18 011110000100101000111010100000110101101100100000000001000011101101010100101111011 x 0111100001110001000100110100110111111101100100000000001000011101101010100101111011
19 001010110101110000010100010011011011111111101001011000100101010101001110000001000 x 00101011010111110000010100010011011011111111101001011000100101010101001110000001000
20 00100101110001011001101111010110101010010000111110001101000011000010011110110010 x 00000101110001011001101111010110101010010000111110001101000011000010011110110010
21 111011001011001110110000000000110011000001101111000010100010111101000110010111011 . 111011001011001110110000000000110011000001101111000010100010111101000110010111011
22 101001101111011010110100000001000011110111111111100110100111001001100001111101010 . 101001101111011010110100000001000011110111111111100110100111001001100001111101010
```



```
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%
fx >>
```

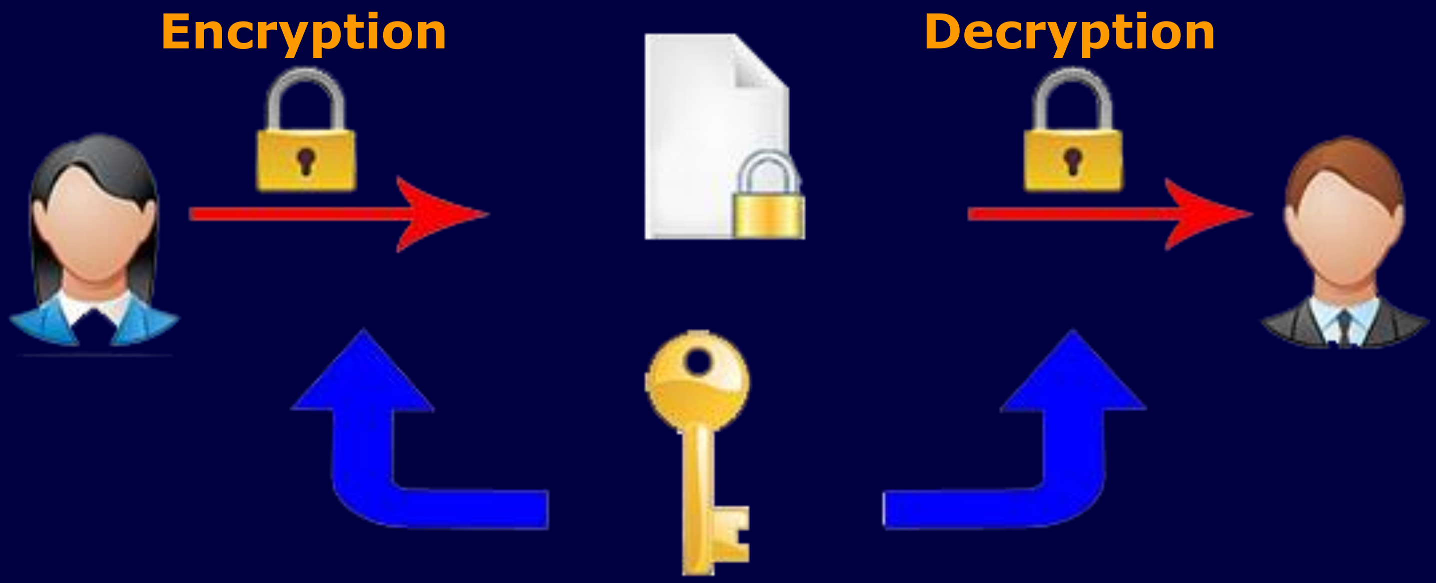
Timing-Based Physical Layer Encryption

Matlab BER Results



Timing-Based Physical Layer Encryption

Application



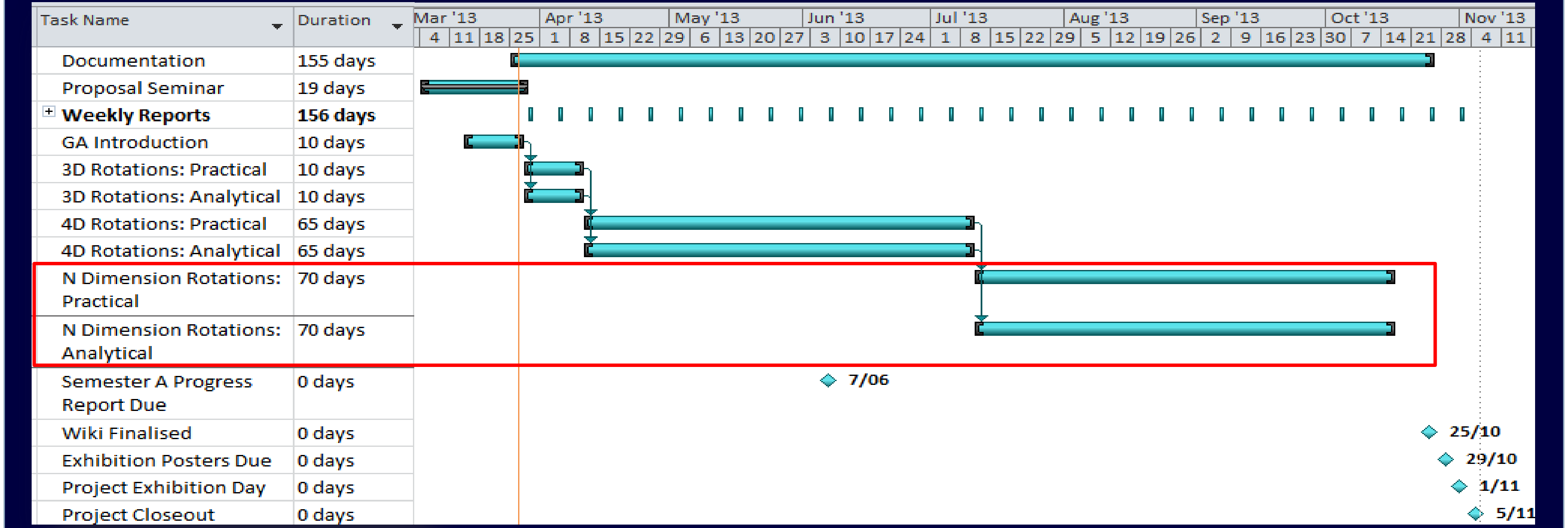
Project Management

Risk Management Evaluation

Risk	Likelihood	Severity	Avoidance/Mitigation Strategies
Unavailability of Team Member	Low	Medium	Both members are well versed in each aspect of the project and the overall progress.
Loss of work	Very Low	Low	Group members will ensure that all progress is shared via the wiki, Facebook and through email so that we have several working copies available.
A Lack of Technical Knowledge	Low	High	We'll need to ensure that we're maintaining communication with each other and our supervisors to make sure that we understand the technical elements of the project
Falling Behind Schedule as a result of the increased complexity of the project.	Low	Medium	Re-evaluate our expectations of the project, and perhaps increase the focus in lower dimensions (such as 4, 5 and 6) before even considering the higher dimensions.
Not finding a solution for keyless encryption	Very High	Very Low	Ensure that out work is completely documented, so that regardless of what we've found we have something to show at the project closing.

Project Management

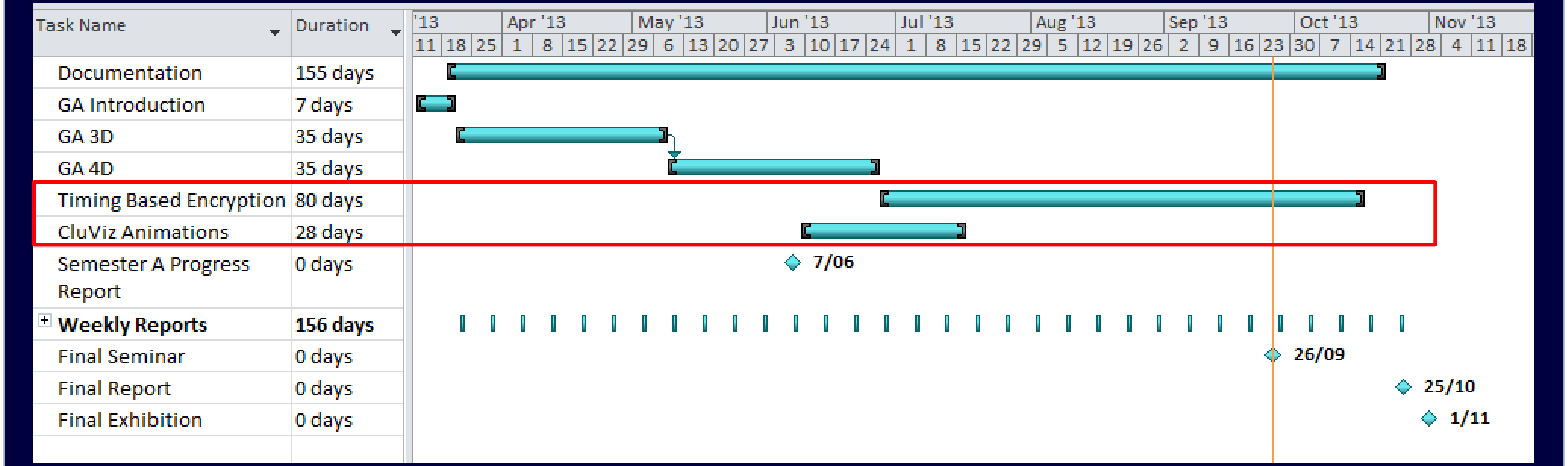
Initial Project Schedule



Task Name	Duration
Documentation	155 days
Proposal Seminar	19 days
Weekly Reports	**156 days**
GA Introduction	10 days
3D Rotations: Practical	10 days
3D Rotations: Analytical	10 days
4D Rotations: Practical	65 days
4D Rotations: Analytical	65 days
N Dimension Rotations: Practical	70 days
N Dimension Rotations: Analytical	70 days
Semester A Progress Report Due	0 days
Wiki Finalised	0 days
Exhibition Posters Due	0 days
Project Exhibition Day	0 days
Project Closeout	0 days

Project Management

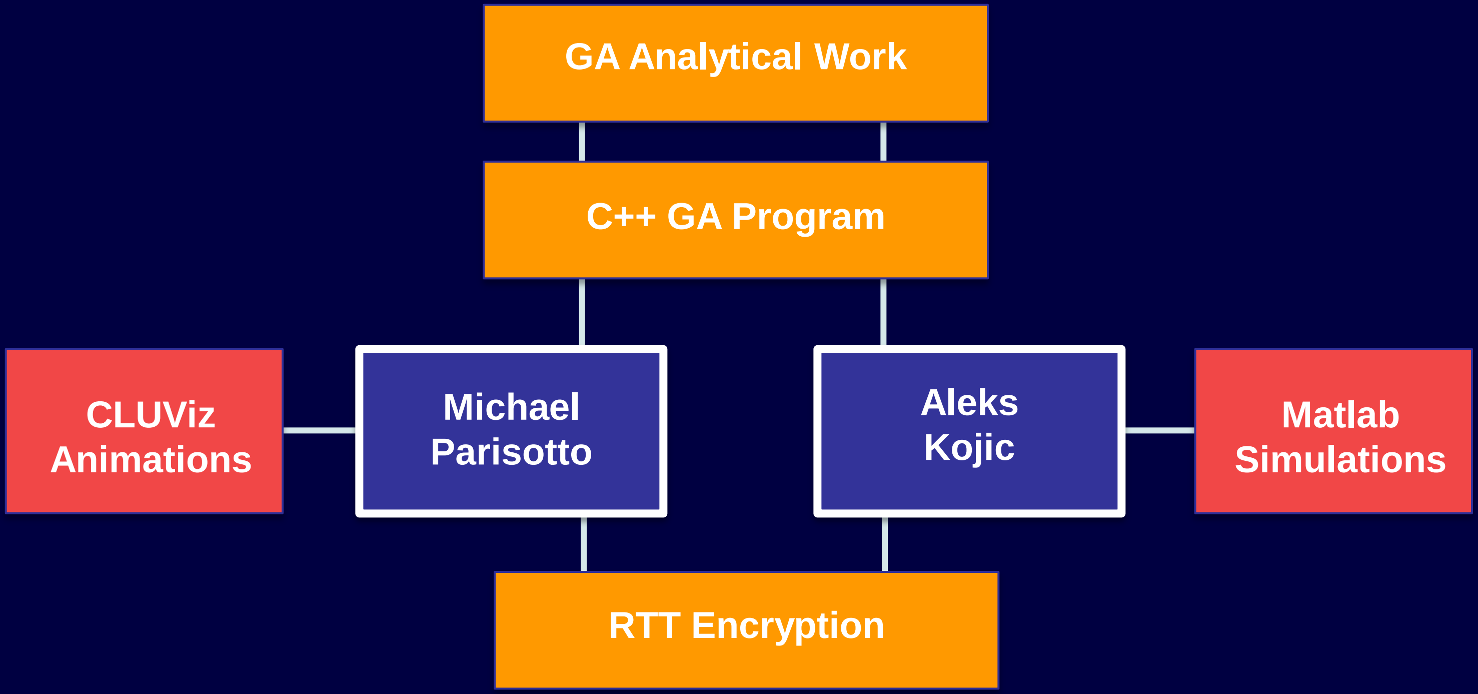
Resulting Project Schedule



Task Name	Duration
Documentation	155 days
GA Introduction	7 days
GA 3D	35 days
GA 4D	35 days
Timing Based Encryption	80 days
CluViz Animations	28 days
Semester A Progress Report	0 days
+ **Weekly Reports**	**156 days**
Final Seminar	0 days
Final Report	0 days
Final Exhibition	0 days

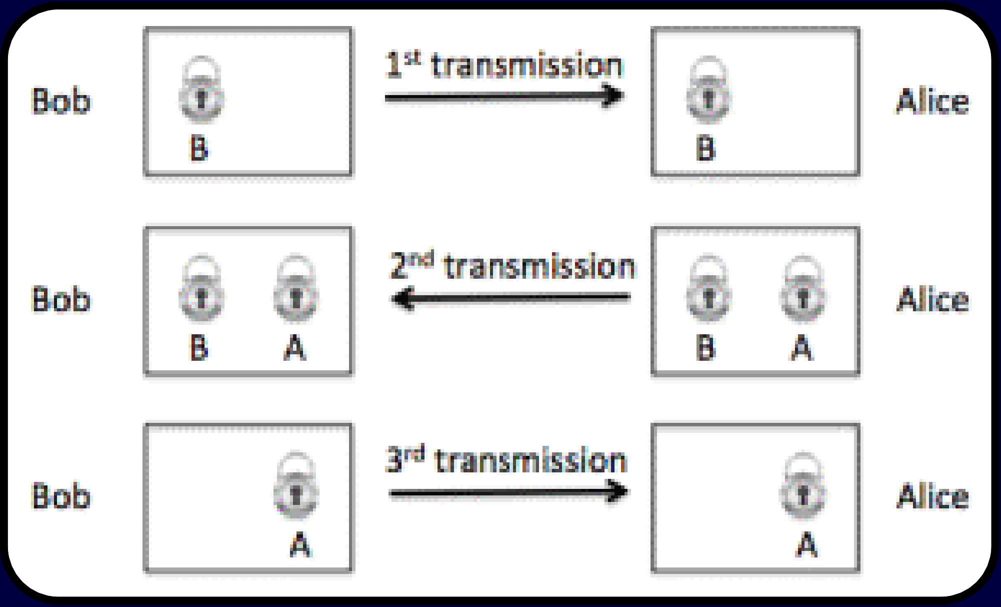
Project Management

Team Management & Organisation



Conclusion

- Geometric Algebra and Physical Timing Based Encryption
  - Appreciation for Cryptography



Thank you for listening

Questions

Key References

[1] L. Kish and S. Sethuraman, ‘Non-breakable Data Encryption with Classical Information’, *http://ee.tamu.edu/~noise/research_files/new_encryption.pdf*

[2] L. Kish and J. Bergou, ‘Absolutely secure QKD Scheme with no detection noise, entanglement and classical communication’, *http://arxiv.org/pdf/quant-ph/0509097.pdf*

[3] L. Gunn ‘Physical-layer encryption on the public internet: a stochastic approach to the KS cipher’, *http://arxiv.org/pdf/1306.4174v1.pdf*

[4] M. Gander and U. Maurer ‘The secret-key rate of binary random variables’, *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=394667*