THE UNIVERSITY of ADELAIDE

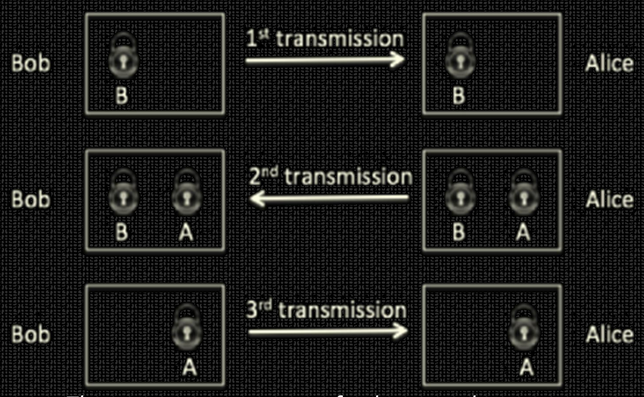
SCHOOL OF ELECTRICAL AND ELECTRONIC ENGINEERING

Secure Communications

Is it possible without a key exchange?

Background & Motivation

The Kish-Sethuraman (KS) cipher, also known as the double-padlock protocol is theoretically known to offer absolute security through a classical information channel. Realization of the protocol remains a difficult problem as the required mathematical operators are yet to be found.



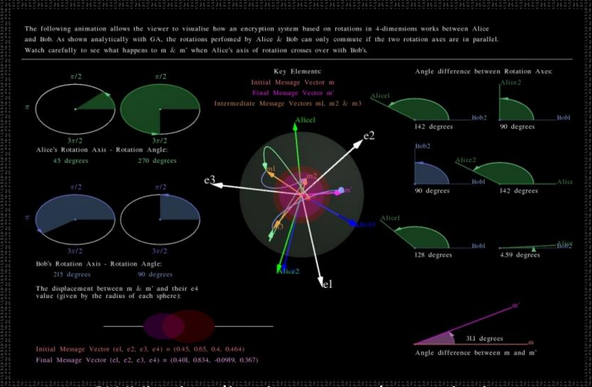
The message appears perfectly secure because at all times it has been secured by at least one lock

Finding a representation for the KS cipher shall enable completely secure communication between two parties and would prove invaluable in fields such as finance, defence and even personal communications.

Methodology

Preliminary investigations using geometric algebra (GA) explored the possibility of encryption via rotations in n-dimensions by stepping up through the dimensions starting with 3D.

We would then identify possible encryption operators and then either confirm or disprove their viability theoretically with the aid of software and developed animations using CLUViz.



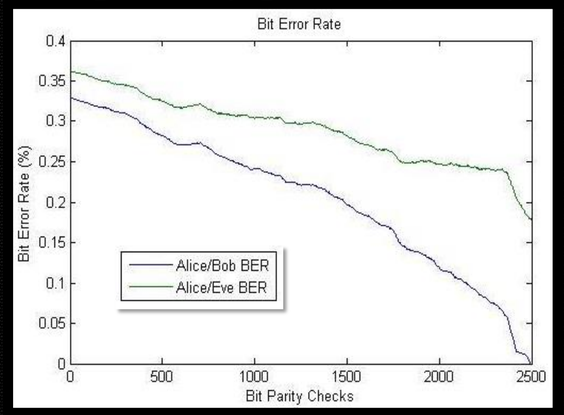
CLUViz visualisation created to assist in understanding rotations in 4-dimensions

Due to complications and a flaw with our initial approach summarised with Information Theory, we moved towards timing-based physical layer encryption as a possible avenue for success.

This method utilises the noise over the communication channel to ensure that an 'eavesdropper' cannot get the same quality of information as the sender or recipient.

Results

A program was created which implemented this timing-based key agreement protocol.



Shows that the BER between the sender and recipient reconciles faster

The program operates by recording the round trip times of the sender/recipient, turning these round trip times into a sequence of bits, and then reconciling the sender/recipients bit stream through bit parity checks.

After initial testing, we reached two main conclusions.

1. Regardless of the operational scenario, whether it be over a LAN network or over the internet, the sender and recipient are able to generate a bit stream which stays in sync.

2. The eavesdropper is never able to get the same quality of information as the sender/recipient when using this protocol, however the effectiveness does vary.

Future Extensions

At the moment, the timing-based key generation protocol generates a secure bit stream for the sender/recipient which they can use as a one time pad for encryption.

It may be of interest in the future for this bit stream to be interpreted as something else to perhaps add another layer of security, much like the bit parity checks do, and improve the protocol.

Students: Aleks Kojic & Michael Parisotto | **Supervisors:** Derek Abbott, James Chappell & Lachlan Gunn

[1] L. B. Kish, S. Sethuraman **"***Non-breakable Data Encryption With Classical Information"* **[2]** D. Abbott, J. Chappell *"The double-padlock problem: is secure classical communication transmission possible without key exchange?"*
[3] L. J. Gunn, D. Abbott, J. Chappell, A. Allison *"Physical-layer encryption on the public internet: a stochastic approach to the Kish-Sethuraman cipher"*