Is secure communications possible?

Yuanhao Liu, Christopher Lau

Supervisors: Prof Derek Abbott; Dr James Chappell; Mr Lachlan Gunn

THE UNIVERSITY of ADELAIDE

Electrical and Electronic Engineering

Project Background

This project seeks to find ways in which two parties (Alice & Bob) are able to securely communicate with each other. Our encryption is entitled 'Timing Based Key Agreement' (TBKA). We propose to generate the key from a common source – the round trip times between two parties and we also introduced two error correction techniques: Parity Iteration Protocol; and Cascade Protocol. This form of encryption only uses classical techniques which makes our encryption technique much easier to deploy into present-day devices than quantum systems.

Bit Stream Generation

Alice, Bob and Eve obtain round trip times, Ta, Tb and Te respectively (see Figure 1). Afterwards round trip times are converted into bit streams for each party (see Figure 2).

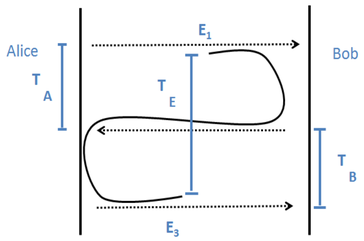


Figure 1 : A visual representation of the round trip times Ta, Tb, and Te

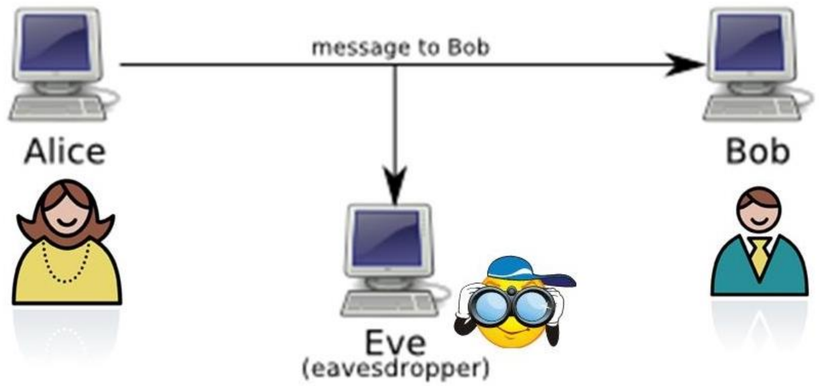
$$\text{if } x > \text{median} \quad \text{bit} = 1$$

$$\text{if } x < \text{median} \quad \text{bit} = 0$$

Figure 2 : The conversion between round trip times and bit stream.

Encryption between Alice and Bob

Random bit streams are generated by Alice and Bob as private key to encrypt our message.



Eavesdropper

Wireshark is used by Eve to capture packages that are transmitted on the network between Alice and Bob.

WIRESHARK

Error Correction Techniques

Parity Iteration Protocol

Alice: 00 11 01 00 — Original bit streams

Bob : 01 11 11 00 — (blocks of 2)

Alice: 0 0 0 0 — Parity check

Bob : 1 0 1 0 — (xor all bits in a block)

x ✓ x ✓

Alice: 11 00 — Corrected bit streams

Bob: 11 00

Cascade Protocol

Alice: 0011 1100 — 00 11 11 00 — 00 11 11 00

Bob : 0111 1100 — 01 11 11 00 — 01 11 11 00

Alice: 0 0 — 0 0 — 00

Bob : 1 0 — 1 0 — 01

Alice: 0011 1100 — Corrected bit streams

Bob: 0011 1100

Results

Comparing the two protocols, Cascade is chosen to be used for error correction and the eavesdropper also uses this protocol. Based on this protocol, Alice and Bob generate the same private key but although uses Eve the same procedure as Bob her key is not the same as Alice or Bob.

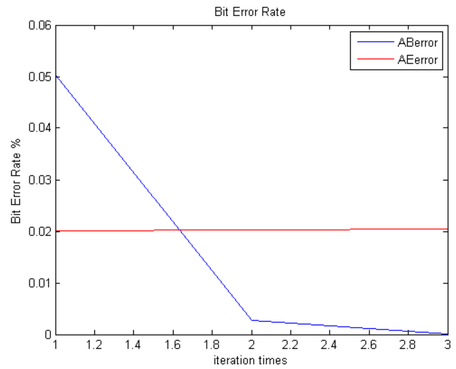


Figure 3 : Simulation of TBKA and using the Parity Iteration protocol

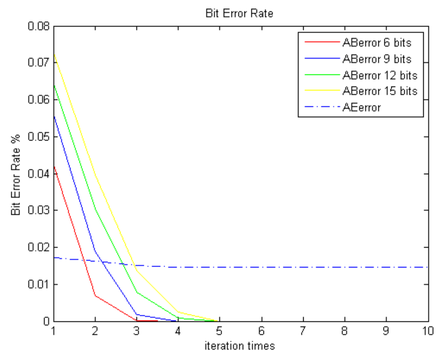


Figure 4 : Shows the performance of Cascade Protocol using different block sizes

Conclusion

Initial results show that this encryption system is promising because the eavesdropper at the moment is unable to fully reconcile her intercepted key. More research needs to be undertaken to determine the capabilities that the eavesdropper requires in order to completely correct her key and to break the encryption system.

References

[1] L. J. Gunn, J. M. Chappell, A. Allison, and D. Abbott, "Physical-layer encryption on the public internet: A stochastic approach to the Kish-Sethuraman cipher," Int. J. Modern Physics, Vol. 33, Art. No. 1460361, 2014

[2] Mateo J. M. et al. 'Demystifying the Information Reconciliation Protocol Cascade', July 2014