MEASUREMENT DEVICE INDEPENDENCE ASPY'S WORST ENEMY

CHRIS IRISH AND JONATHAN GOUGH DEPARTMENT OF PHYSICS AND ASTRONOMY



INTRODUCTION

Introduction Introduction

QUANTUM KEY DISTRIBUTION

Quantum Key Distribution Quantum Key Distribution

REFERENCES

[1] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. *Phys. Rev. A*, 54:2651–2658, Oct 1996.

ALICE HAS A SECRET



MEASUREMENT DEVICE INDEPENDENCE

Alice and Bob are sick of having their secrets found out by Eve. Bob suggests they try a new approach, *Measurement Device Independent Quantum Key Distribution*. Instead of sending there secrets directly to each other, they send them to a third party (Charlie). Charlie can combine Alice and Bobs information and perform a operation unique to quantum physics, called a Bell Measurement. The bell state measurement provides a vital piece of information that when combined with Alice and Bobs information, it allows them to work out what information is being sent to them. As only Alice/Bob knows her/his outgoing information, only they can know what information is being passed through the network.

However Bob has had one to many cranberry juices/Barnsley Bitters and can no longer remember what he sent to Alice. Just like Eve, Bob is now locked out of the network as Charlie can no longer verify him as a network user. Silly forgetful Bob!

