Measurement Device Independence
Eve's worst nightmare

Chris Irish and Jonathan Gough
Department of Physics and Astronomy

Alice Has A Secret

It started with a secret. Alice "found" a wholesale box of Monster Munch behind the UCL cafeteria, and quickly stashed it in some bushes. She wanted to share it with Bob, as she'd never manage the entire box herself, but had to be careful, or she might have to share with everyone else too! She sent an **encrypted message** to Bob, to share the amazing news, but the joy would soon turn sour. Bob called back shortly afterwards - he'd been to the drop, but every one of the delectable maize snacks had vanished! They realised their secret **encryption key** had been cracked, and it could only be one person: **Eve the eavesdropper**. Eve loves to learn people's secrets and share them with everyone, and Alice is the perfect mark. Alice and Bob need a method to tell when Eve is listening in on their conversations, luckily Bob's been reading the latest issue of cryptographic weekly and thinks he may have the answer. They needed **Quantum Key Distribution**!

Quantum Key Distribution

Luckily, UCL had some suitable components lying around, and a spare **fibre-optic network**, spanning important sites such as IT, the Library, and McDonald's. With QKD in place, Alice sent photons of light, polarised in different directions to represent binary bit values (0 or 1) of the **encryption keys**. They would switch their instruments randomly between two **bases**, so that if you measured in the wrong basis, you would get a random value, and you couldn't be sure if anything was correct. Eve's also been reading the latest issue though and is familiar with the dark arts of quantum hacking, and wouldn't be put off so easily. She intercepted and measured some of Alice's photons, and prepared new photons to send on to Bob. Alice and Bob were clever though. They shared some of the results on the phone, with Eve listening in, and managed to spot the wrong bits, or **bit errors**, caused when she'd guessed incorrectly.

Eve was rumbled, it seemed all was lost. But another flick through the latest cryptography weekly gave her new hope - she just had to be extra sneaky to exploit the **loopholes**. Alice's signal would experience interference from the environment, and the further it travelled, the more bit errors were introduced. Errors also occurred due to their equipment gradually starting to point the wrong way, or becoming misaligned. The errors caused by Eve's interactions became harder to spot. Eve learned to cleverly manipulate the signal to put Alice and Bob's equipment a little out of sync without them realising, providing extra cover for her attacks. Worse still, distances of over a few km, such as from the library to McDonald's, weren't possible without using a relay to pass on the signal. This relay Eve could easily hack, and control.

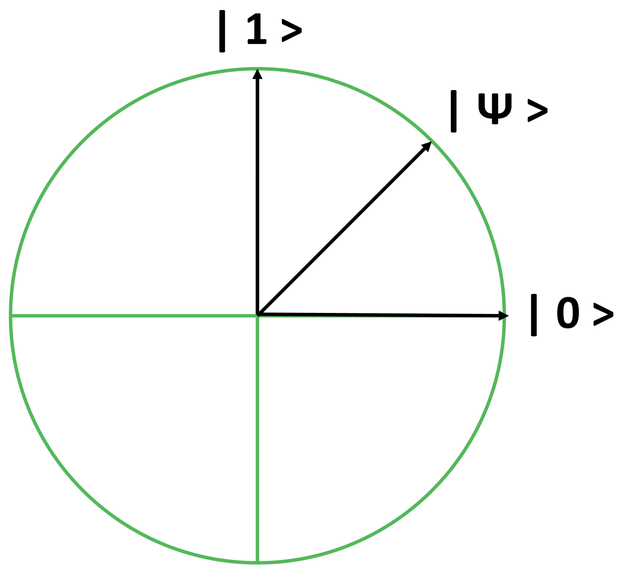
Even as Alice transmitted the entire contents of her little sister's diary, she didn't talk for fear of discovery. But when Alice confessed that her favourite Love Island contestant was Curtis, Eve just couldn't be quiet any longer, and humiliation soon followed.

References

[1] Yan-Lin Tang, Hua-Lei Yin, Qi Zhao, Hui Liu, Xiang-Xiang Sun, Ming-Qi Huang, Wei-Jun Zhang, Si-Jing Chen, Lu Zhang, Li-Xing You, Zhen Wang, Yang Liu, Chao-Yang Lu, Xiao Jiang, Xiongfeng Ma, Qiang Zhang, Teng-Yun Chen, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Phys. Rev. X*, 6:011024, Mar 2016.

Map

Definitions



Encryption key: A secret sequence of characters that can be used with a program to scramble text in a unique way, so that it can only be unscrambled if you know the full sequence.

Basis/bases: Just as we can *decompose*, or break-down, a line on a graph into a simple set of x- and y-coordinates, we can decompose polarisation into a combination of simple units, each called a "base", for instance "horizontal" or "vertical". A full set is called a "basis", plural "bases", which confusingly is spelled the same as the plural for "base", but pronounced "bay-sees".

Qubit: A 2D quantum system represented in the *computational basis*.

Bell Measurement: A joint measurement performed on a two qubit state that expresses correlations between the qubits.

Measurement Device Independence

Alice and Bob are sick of having their secrets discovered by Eve. Bobs been reading the newest issue of cryptographic weekly and discovers a new approach, **Measurement Device Independent Quantum Key Distribution**. Instead of sending their secrets directly to each other, they send them to a third party, there friend **Charlie**. Charlie can combine Alice and Bob's **information** and perform an operation unique to quantum physics, called a **Bell Measurement**. The bell measurement provides a vital piece of information that when combined with Alice and Bob's data, allows them to work out what is being sent. As only Alice/Bob knows her/his outgoing data, only they can know what information is being passed through the network.

In celebration of finally having a secure network, Bob has had one too many pints and can no longer remember what he sent to Alice. Just like Eve, Bob is now locked out of the network, as he can no longer work out what Alice is sending him. Silly forgetful Bob!

Dr Lluis Masanes - MDI Expert at UCL