NEWS & TECHNOLOGY 17 January 2018

Clever maths will stop hackers spying on the quantum internet

By **Jacob Aron**

THERE'S a new way to make sure quantum networks are secure.

Theoretically, messages sent via quantum networks are protected by the laws of quantum mechanics. This is because any attempt to intercept information sent between two parties will disturb its fragile quantum state, revealing the eavesdropper. One way to check a quantum line is secure involves solving an equation called a Bell inequality – if the result exceeds a certain number, there is a limit to how much information a spy can extract without being detected.

But this is only true for messages sent between two points. On a more complex network, the Bell inequality doesn't apply. That is roughly because quantum hackers can gain a little bit of information from each part of the network and then piece it together. One solution would be to create point-to-point connections between everyone on a quantum network, but that is hardly practical, says Ciarán Lee at University College London.

Lee and his colleague Matty Hoban at the University of Oxford have found a better way. They have shown that a more complex version of the Bell inequality can provide the same security assurances for a network as the simpler version does for point-to-point contact. There is just one problem: figuring out what this equation looks like is very difficult.

The pair overcome this by using a technique from machine learning called causal inference to study the structure of the network. Essentially, a computer analyses the direction of information flow between the different nodes to figure out its causal structure. For example, if node A is connected to node C via node B, A and C can't communicate unless the message goes via B first (*Physical Review Letters*, doi.org/ch89).

Knowing this structure lets the pair come up with a Bell inequality for any kind of network, which can be used to guarantee its security.

This article appeared in print under the headline "Unhackable quantum comms for all"

---

this article.

Magazine issue 3161, published 20 January 2018