PHYS.ORG

How to decide who keeps the car: Tossing quantum coins moves closer to reality

November 29 2011

Alice and Bob have broken up and have moved as far away from each other as possible. But they still have something to sort out: who gets to keep the car. Flipping a coin while talking on the phone to decide who gets to keep it just won't work. There's no trust. Neither believes each other's result.

A paper published in *Nature Communications* by a team of researchers from Canada and Switzerland explores the concept of coin flipping in the context of quantum physics that uses light particles, so-called photons, to allow communication tasks in a manner that outperforms standard communication schemes.

To understand the researchers' approach, it helps to use an analogy that involves a safe. Bob flips a coin and sends the result of his coin flip, hidden in the safe, to Alice. Upon receiving Bob's safe, Alice sends the result of her own flip to Bob. Once received, Bob sends the key to Alice who unlocks the safe. Now, Alice and Bob both know each other's coin flip and, according to some previously agreed-upon rule, who will drive away with the car.

In a world made out of electronic bits, used for communication instead of safes, the physical safe is replaced by encryption over email. This procedure is believed to be hard to break. Unfortunately, no one knows if this is truly a good safe. This would allow Alice to cheat by unlocking Bob's "safe" without awaiting his key, reading the secret, and choosing the result of her own flip in a way that ensures that she will keep the car.

But it's a different story with quantum communications.

"What we have shown here is the first implementation of quantum coin flipping in which a cheater can not take advantage of the fact that photons may get lost during transmission between Alice and Bob. All previous quantum communication schemes could be broken by a cheater," says co-author Dr. Wolfgang Tittel, professor in the Institute for Quantum Information Science and the Department of Physics and Astronomy at the University of Calgary. The other co-authors are from the University of Calgary, Université de Montréal, École Polytechnique de Montréal and Université de Genève, in Switzerland.

The quantum coins in this study were tossed with one player being at the University of Calgary and the other player at the SAIT Polytechnic, roughly 5 km apart.

"The exchange of quantum bits instead of electronic bits prevents unrecognized cheating because we base our protocol on properties of nature, such as the impossibility to perfectly determine the quantum state of a single photon" say Dr. Félix Bussières, who did parts of his PhD studies at the University of Calgary, where the experiment was performed, before moving to Switzerland to take up a postdoctoral fellowship.

"Unfortunately, even in the quantum world, coin flipping at a distance is not perfect either - it is still possible to cheat, at least to some extent. However, no party can fix the final outcome with certainty, and, if trying to cheat, risks being caught cheating."

Nevertheless, this demonstration has made the decision of who gets the car fairer.