

# Could some entangled states be useless for quantum cryptography?

5 July 2010, By Miranda Marquit

(PhysOrg.com) -- One of the widely accepted properties of quantum entanglement is secrecy. Since scientists and researchers began working with quantum key distribution, entanglement has been considered an essential part of keeping communications private. What if entanglement didn't always mean secrecy, though? New work is shedding light on the nature of entanglement and quantum key distribution - and possibly proving that a high degree of entanglement does not necessarily lead to complete secrecy.

"Entanglement, or quantum correlation, is responsible for enabling quantum key distribution, a method to distribute a perfectly secret key that can be used to encrypt messages," Matthias Christandl tells *PhysOrg.com* via email. "We have now discovered that not every type of entanglement is useful for quantum key distribution... [W]e showed that sometimes particles can be very strongly entangled, but at the same time be nearly useless for cryptography!"

Christandl is a scientist who recently moved from the University of Munich, Germany, to ETH Zurich, Switzerland. Christandl worked with Norbert Schuch at the Max Planck Institute for [Quantum Physics](#) in Garching, Germany, and with Andreas Winter at the University of Bristol in the U.K. and the National University of Singapore to illustrate an example of a [quantum state](#) that is entangled, but that does not offer the secrecy needed for [quantum cryptography](#). Their work appears in [Physical Review Letters](#): "Highly Entangled States with Almost No Secrecy."

So far, the findings are only a theoretical observation. "We studied the possibilities that the world of single atoms and weak bursts of light offers when security is concerned," explains Christandl. The two particles that are used in this theoretical exploration are in what Christandl calls an "antisymmetric state."

Observing this [entangled state](#) in the laboratory may not be something that occurs anytime really soon, though. "This state may be difficult to create in the laboratory," says Christandl, "as one needs a high number of maximally entangled particles in order to create the state. ...However, the insights gained in this work might offer a route to new and better protocols for quantum cryptography."

Christandl and his colleagues are looking at ways to better understand how secrecy works in quantum physics. The idea that, theoretically, even high degrees of [quantum entanglement](#) may not lead to complete secrecy, could change the way that scientists view quantum cryptography. It could also encourage the study of different quantum states to determine which are better for [quantum key distribution](#), and which should be avoided for such purposes.

While there are no plans to set up an experiment to test this idea, Christandl thinks that the theoretical findings can help advance the study of quantum physics. "A better understanding might lead to novel quantum protocols and quantum technologies in the future."

The next step for Christandl and his peers is to look for entanglement that offers no secrecy. "This would push our findings to the extreme," he says, "offering an analog of the famous 'bound entanglement.' Such a finding would conclusively revise the view that entanglement and secrecy go hand in hand."

**More information:** Matthias Christandl, Norbert Schuch, and Andreas Winter, "Highly Entangled States with Almost No Secrecy," *Physical Review Letters* (2010). Available online: [link.aps.org/doi/10.1103/PhysRevLett.104.240405](http://link.aps.org/doi/10.1103/PhysRevLett.104.240405)

Copyright 2010 PhysOrg.com.  
All rights reserved. This material may not be

published, broadcast, rewritten or redistributed in whole or part without the express written permission of PhysOrg.com.

APA citation: Could some entangled states be useless for quantum cryptography? (2010, July 5) retrieved 27 February 2021 from <https://phys.org/news/2010-07-entangled-states-useless-quantum-cryptography.html>

*This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.*