Geneva brings quantum cryptography to Internet voting

By Ryan Paul | Published: October 12, 2007 - 10:47AM CT

Geneva, Switzerland, has long been at the forefront of electronic voting innovation. In 2004, Geneva rolled out one of the first Internet voting systems in the world. Now Geneva is touting its new unique electronic voting security system that uses quantum cryptography to guarantee against eavesdropping.

Developed by id Quantique in collaboration with the Australian company Senetas, the Cerberis quantum cryptography system will be used to protect election data relayed over a fiber optic connection. Unlike conventional Internet cryptography protocols, which use public key infrastructure, quantum cryptography relies on the principles of quantum uncertainty and generally involves encoding information into photons in a manner that will be noticeably and irreparably disrupted by any form of interception or monitoring. The cryptographic technique is still considered radically experimental, and this is one of the first practical applications of the technique.

Under ideal circumstances, quantum cryptography can ensure that communications between two parties have not been overheard. In the real world, however, quantum cryptography is subject to a number of different attacks. At present, any particle system is probably immune to such attacks because of the technical knowledge required to carry one out.

"We would like to provide optimal security conditions for the work of counting the ballots," said Geneva state chancellor Robert Hensler in a statement. "In this context, the value added by quantum cryptography concerns not so much protection from outside attempts to interfere as the ability to verify that the data have not been corrupted in transit between entry and storage."

The technology was originally developed by Professor Nicolas Gisin at the University of Geneva, before id Quantique was formed to continue pursuing the project. "[P]rotection of the federal elections is of historical importance in the sense that, after several years of development and experimentation, this will be the first use of a 1GHz quantum encrypter, which is transparent for the user, and an ordinary fiber-optic line to send data endowed with relevance and purpose," Gisin told Nanowerk News.

Although Geneva's use of innovative new quantum cryptography technology to secure the relay of sensitive election data is very impressive, there are still fundamental flaws in electronic voting that threaten to undermine the integrity of elections. Voter verifiable paper trails and consistent election auditing practices are needed to ensure that the process remains effective and transparent. Using quantum cryptography to lock down one step in the election data chain of custody is a promising contribution to election integrity, but the rest of the process is still subject to the same old problems.