PHYS.ORG

New Quantum Strategy Keeps Web Searches Private

June 27 2008, By Lisa Zyga

When an Internet user types a word or phrase into a search engine, the Web server has the ability to find out that inquiry. As more people and businesses are becoming concerned about privacy, researchers are developing new ways to make online activity more secure for both users and servers.

Recently, physicists have created a cheat-sensitive protocol called quantum private queries (QPQ). The quantum-based system allows a user to search for and retrieve an item from a database without revealing that item to the server. If the server tries to find out the item, the user can tell, and modify their use accordingly.

The server is also protected because the user can only retrieve a limited amount of information in a single query, so the server doesn't have to reveal its entire database. Compared with other strategies, the QPQ can provide a much simpler private information retrieval tool in terms of both communication and computation.

The QPQ developers, Vittorio Giovannetti from Scuola Normale Superiore in Pisa, Italy; Seth Lloyd from MIT in the US; and Lorenzo Maccone from Universita Pavia in Pavia, Italy, have published the details of the protocol in a recent issue of Physical Review Letters.

"In simple terms, you may say that the main advantage of the protocol is that it allows us to perform a task that, as far as we know, would not be possible to achieve by classical means: that is, it guarantees both user and data privacy without requiring any costly communication and computational overheads," Giovannetti told PhysOrg.com. "Furthermore, QPQ does not require (at least in its basic implementation) Alice [the user] to use complex encoding of her queries (e.g. to send half of an entangled state to Bob [the server]) nor Bob to perform 'too complex' quantum data processing.

"The prototypical example is, of course, Internet Web search (say Alice wants to know the Internet addresses of the stores that sell cookies in her town, but she doesn't like Google guys to determine what she is really interested in). Other examples could be related to remote bank account checking."

As the physicists explain, the QPQ strategy is designed to protect the user's privacy and the server's information. Normally, these two goals are in conflict, since complete privacy for one side means vulnerability for the other. But QPQ takes advantage of elements of quantum theory to provide a compromise.

In the QPQ strategy, the user Alice performs a search query, and receives a limited number of answers from the server Bob. If Alice suspects that Bob is trying to figure out her queries, she can perform a search query that is a quantum superposition of different queries. Her answer from Bob will reveal whether the superposition has been altered or not, and she will know if he has been trying to read her queries.

In order for the strategy to work, Alice must send her queries in random order, one at a time. This way, Bob doesn't know if a query is a normal query or a superposition query intended to detect his attempts at cheating. Sending queries one at a time prevents Bob from making joint measurements, which might go unnoticed.

Although Bob may be lucky and successfully determine one of Alice's queries by choosing to intercept the normal query instead of the superposition of queries, chances are that he will get caught sooner or later. In fact, the physicists showed that, no matter what sophisticated methods Bob might use to try to intercept Alice's queries, she will likely discover his attempts.

The researchers explain that the QPQ strategy is similar to quantum cryptography, in that both methods provide privacy by enabling the user to perform actions to determine possible interception attempts. Then, the user can take measures to guarantee their privacy in the face of these attempts. Overall, the QPQ protocol provides the same degree of privacy as quantum key distribution, with greatly reduced complexity.

“There are several possibilities [that Alice might use to maintain her privacy when using a dishonest server],” Giovannetti explained. “You can imagine, for instance, a scenario in which there are several providers (say Google, Altavista, etc.) which allow QPQ service at a certain cost per quantum message.

“Now suppose that the customers of a given provider are keeping it under control by posting its honesty rate on a public website: in order to stay on the market, a provider with a low honesty rate will be forced to lower the cost of its QPQ service, i.e. it will allow for more QPQ messages per query. This will allow the customers of the dishonest provider to maintain a sufficiently high privacy by protecting their queries by sending more complex quantum superpositions at the same price they query more honest providers.”

More information: Giovannetti, Vittorio; Lloyd, Seth; and Maccone, Lorenzo. “Quantum Private Queries.” Physical Review Letters 100, 230502 (2008).

Citation: New Quantum Strategy Keeps Web Searches Private (2008, June 27) retrieved 19 April 2024 from https://phys.org/news/2008-06-quantum-strategy-web-private.html