An oblivious transfer protocol for quantum cryptography

1 July 2008, By Miranda Marquit

“It's hard to beat the noise that you have with quantum information,” Barbara Terhal tells PhysOrg.com. “So our security protocol relies on the fact that storing quantum bits noiselessly is hard to do with current technology.”

Terhal is a scientist working at the IBM Watson Research Center in Yorktown Heights, New York. She collaborated with Stephanie Wehner and Christian Schaffner at CWI in Amsterdam on this project that is designed to provide a proof of principle for a form of cryptography known as oblivious transfer. Their work is published in *Physical Review Letters*: “Cryptography from Noisy Storage.”

Quantum cryptography, as first proposed by Charles Bennett and Gilles Brassard in 1984, Terhal explains, “is a protocol for two parties to generate a random bit string such that no third party knows the values of the bits. The random bit string can then be used as a key to send a secret message. The message is encrypted with the key by the sender and decrypted using the key by the receiver. This quantum technology has been realized now.”

Terhal and her co-workers propose to implement a different cryptographic protocol called oblivious transfer using quantum information. “We prove the security of our protocol under the assumption that one cannot yet store quantum information noiselessly,” Terhal says.

“In an oblivious transfer,” Terhal explains, “the sender Alice has two bits. The goal of the protocol is to transmit one of these bits to a receiver Bob, such that Bob determines which one he gets, but Alice does not know which one he gets. In addition, Bob is not allowed to learn anything about the other bit that Alice has.”

Terhal points out that oblivious transfer is used when one of the parties might be dishonest: “For example Bob can try to learn both bits. In the protocol Alice encodes two bits in quantum states. Because Bob cannot reliably store these qubits, he is forced to measure the qubits. The quantum encoding, similar as in the Bennett-Brassard scheme, ensures that he can learn – at most – one of the bits.” If he decides to store the qubits anyway, Terhal and her peers show that the noise involved in the storage will prevent Bob from learning the bits as well.

The main interest in oblivious transfer stems from the fact that the protocol can provide a basis for secure identification. Terhal offers a real-world application for oblivious transfer: “There are many scams that have to do with ATMs. You stick in your card, and you may give away your password. With a cryptographic scheme based on oblivious transfer, you won’t give your password away to a fraudulent ATM. The bank ATM needs to test that you know the password, and you need to test whether the bank knows your password, which it should if it is a proper ATM. With this protocol, the password isn’t explicitly exchanged, but it is established that both you and the bank know the password.”

The oblivious transfer protocol has not been made to work yet. However, Terhal and her colleagues think that their theory, using a model that assumes noisy storage, constitutes a proof of principle that could lead to oblivious transfer in practice. “It’s more of a theory right now,” Terhal admits. “It’s really a security proof that offers first principles that you can build something.”

“There are people working on better quantum memory and storage, in particular for photonic qubits which can be used in this protocol,” Terhal says, “but we wanted to create a protocol that is derived from current technology. We’re using the fact that quantum storage is noisy.”