Backgrounder

Quantum Key Distribution

Systems Security Lab

Quantum Key Distribution (QKD) was developed in HP Labs Bristol to protect against the kind of credit card fraud typical of mail order and online transactions. The prototype system uses a shared secret, a one-time pad, stored in a personal handheld transmitter that could be regularly topped up by secure key exchange with a stationary receiver unit – housed in an automated teller machine (ATM), for instance.

Quantum cryptography provides a means for two parties to generate securely shared secret material. This means that the two parties can amplify an initial store of shared secrets, which may be used in three primary ways:

- to protect the Quantum Key Distribution (QKD) algorithm itself in order to generate new shared secrets,
- to identify themselves to each other, and
- to act as an encryption key to encrypt classically messages being sent between themselves.

Editorial contact:

Julian Richards, HP
+44 (0)117 312 7625
+44 (0) 777 570 1800
julian.richards@hp.com

The QKD prototype is a low-cost, free-space quantum cryptography system using off-the-shelf components that is able to generate and renew shared secrets on demand over a short range of up to one metre in shaded daylight. The transmitter and receiver unit uses a compact diffraction optical element design that the researchers plan to incorporate within a hand-held device such as a smart card or mobile phone.

The system uses the well-known BB84 protocol. The design philosophy is based on a future handheld electronic credit/debit card, which communicates with consumer outlets, such as an ATM, using free-space optics. This device then also acts as a store of secrets shared only with the bank (or central secure server) which can be used to protect online transactions.

With QKD protecting the interface between the ATM and the user's handheld device, there is no possibility of an eavesdropper gaining the secret key information through 'skimming' attacks, in which the key and card details are read using a false front on the ATM itself.

Thanks to QKD, no hacker attempting to read the key could do so without leaving evidence of their efforts, which the user and their bank could detect. If the system were hacked, the user can dispose of the unused keys without compromising personal data. The hacker is left with nothing.

A full software system has been developed to handle synchronization, error estimation and correction and privacy amplification.

Currently, the system can generate around 10,000 bits of secret keys from a one-second

interaction between transmitter and receiver in daylight conditions.

The research team is working to produce stand-alone modules for the transmitter and receiver. An inexpensive field programmable gate array (FPGA) will be used to replace much of what has been achieved by software on the transmitter's computer, as well as replace the driver circuit.

The FPGA transmitter module could be added to a handheld device, such as the HP iPAQ, using infra-red or Bluetooth® wireless technology as the QKD channel.

Bluetooth is a trademark owned by its proprietor and used by Hewlett-Packard Company under license.

© 2008 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.