Quantum Computing:
Report on Quantum Cryptography

Scott Schoeller

1 Principles of Cryptography

A symmetric cryptosystem is defined in the reading [1] as follows: There is a finite set of possible plaintexts (P), another finite set of possible ciphertexts (C) and a finite set of possible keys (K). For each possible $k \in K$, there is an encryption rule and a decryption rule corresponding to that encryption rule. The decryption rule is defined such that $d_k : C \to P$. The encryption rule is defined as the reverse of the decryption rule. Asymmetric encryption utilizes the concept of a "shared secret." Asymmetric encryption, such as Diffie-Hellman and RSA cryptosystems, is the focus of the paper, since this is the type most susceptible to being broken by a quantum computer.

2 Deficiencies of Classical Methods

Most transposition and substitution ciphers are vulnerable to both quantum and classical attacks. Prominent asymmetric classical methods (RSA, ElGamal) don't have definitive proofs of security. In particular, the computational hardness and one-way properties have not been fully proven. Additionally, classical asymmetric techniques are vulnerable to attack via Shor's Algorithm.

3 Quantum Cryptography

The challenge of potential breakage of current asymmetric cryptography also provides opportunity for new methods.

3.1 Key Distribution

In quantum key distribution, a quantum channel is utilized for transfer of the shared key as qubits. The reading mentions the BB84 protocol. Two versions of this protocol exist: "prepare-and-measure" and an entanglement-based version. Both are equivalent. The prepare-and-measure version works as follows. Alice prepares 2n qubits randomly and then sends them to Bob. Bob randomly measures each qubit in one of two bases. Alice tells Bob over an insecure channel which basis was used. The error rate can be estimated with classical methods.

3.2 Unconditionally Secure Quantum Bit Commitment

The problem of "unconditionally secure quantum bit commitment" is as follows: can someone create a message, encrypt it via quantum methods and make the encoded message both unreadable and unalterable by the original sender? This problem is computationally impossible to solve.

References

[1] Dagmar, B., Erdelyi, G., Meyer, Tim, Reige, Tobias, and Rothe, J. Quantum cryptography: A survey. *ACM Computing Surveys 392*, 2 (June 2007).