Reading Journal for PRISM 2024

1 Software Security

2 Cryptography

Quantum Cryptography and Security Analysis by Babber & Singh

Summary

This paper briefly overviews the current state of non-quantum cryptographic algorithms and then proposes Quantum Key Distribution (QKD) as a quantum-attack-resistant alternative. It explains that our current cryptosystems (like RSA or Diffie-key exchange) will be vulnerable to attacks since they rely on integer factorization or discrete log problems, which quantum computers can solve quickly. On the other hand, QKD promises "an infallible secure transmission of data." The authors propose a simple common key structure that works by prepending the number of 0s in the message and appending the number of 1s in the message to our actual binary message before transmission. This cryptosystem ensures security by exploiting quantum physics's uncertainty principle and no-cloning property. As the number of photons transmitted increases, the probability of detecting a malicious actor approaches 100%. While the actual transmission of data is not the main focus of this paper, it works by sending a series of photons by laser through the atmosphere or fibre optic cable.

Strengths & Weaknesses

The paper does a fantastic job of providing a broad survey of existing algorithms Since nature of a survey style paper like this one means that it leaves a lot to be desired in terms of specificity.

Potential Significance

3 Computing and Society