Reading Journal for PRISM 2024

1 Software Security

2 Cryptography

"Quantum cryptography and security analysis" by Babber and Singh [1]

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 the existing algorithms and proposing a new one as a solution to the rise of quantum computers. However, due to its nature as a survey-style paper, it misses more precise details about QKD's actual implementation. While that may not be within this paper's purview, I feel it is something we should consider. Some (possibly elementary) questions I have are:

- Why do we need a common encryption/decryption scheme, and if Diffie-Hellman key exchange is vulnerable how do I send that scheme?
- While the paper proposes QKD as theoretically immune to eavesdropping are there practical limitations to this once QKD is implemented in the physical wolrd?

Potential Significance

While this paper will be very useful if we focus on something on the advent of quantum computing and its impact on cryptography, it is true that it does not explicitly address any questions of computing and society. Still, if we choose to focus on that area, it will be helpful as it provides a sound but digestible technical overview of the current state of quantum cryptography. Either way, if possible, we should complement this paper with something more specialized.

3 Computing and Society