Vinzenz V., Viola H. *Quantum Hacking* *21. April 2015*

Abstract

One simple way to securely encrypt a message is the one-time-pad. This method came up in the early 20th century and played an important role during the cold war. It can be proven that, if the following three assumptions hold, it is impossible to decrypt the message encrypted with a key. The assumptions are (1) truly randomness of the key, (2) single use of the key and (3) secure transmission of the key. The latter will be the problem we will refer to in our talk. One solution to this is the Quantum Key Distribution (QKD).

In our talk we will mention the most important QKD protocols and will discuss the BB84 in more detail, since we will need it, to understand how the later explained hacking works.

Eventually we will explain how commercially available quantum systems where hacked. Therefore we will refer to the paper by Lars Lydersen et. al. 2010 and present the trojan horse attack. We will point out how the attack was technically implemented and at what kind of loopholes the attackers exploited with their hack.