ulm university universität
uulm

Einladung
zum
Physikalischen Kolloquium

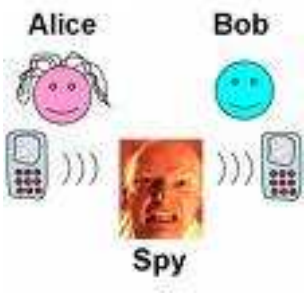
Montag, 31.05.2010,
16.15 Uhr im H2 (025)

Prof. Dr. Artur Ekert
Quantum Physik, Mathematical Institut
University of Oxford, UK

Is there a perfect cipher?

Human desire to communicate secretly is at least as old as writing itself and goes back to the beginnings of our civilisation. Over the centuries many ingenious methods of secret communication have been developed, only to be matched by the ingenuity of code-breakers. As the result, the quest for a perfect, unbreakable, cipher, had been declared a futile pursuit. That is, until recently! Surprisingly, a combination of quantum physics and cryptography promises to dash the hopes of would-be eavesdroppers, perhaps for good. Code-makers, it seems, may have beaten code-breakers at last.

In my talk I will focus on the quest for perfect secrecy. I will describe how people tried to protect communication in the past, how it is done today, and I will speculate how it may be done in the future. Physics plays increasingly more important role in this field simply because the process of sending and storing of information is always carried out by physical means. In particular, eavesdropping can be viewed as a measurement on a physical object, in this case the carrier of the information. What an eavesdropper can measure, and how, depends exclusively on the laws of physics. I will explain how, using quantum phenomena, physicists managed to design and to implement a system which is regarded to be unbreakable. Moreover, recent research shows that security of communication can be guaranteed by peculiar "non-local" correlations, no matter whether they are of quantum origin or not. Bell's inequality alone makes seemingly insane scenario possible---devices of unknown or dubious provenance, even those that are manufactured by our enemies, can be safely used for secure communication. This is a truly remarkable feat, with a number of significant contributions from ICFO researchers. I will provide a brief overview of the intriguing connections between Bell's inequality and cryptography.



Organisation: **Prof. Ankerhold, Tel.: - 22913**
Prof. Hecker Denschlag, Tel.: - 26100
Host: **Prof. Calarco, Tel.: - 22832**