

**Position Paper**  
to the  
**STORK Cryptography Workshop:**  
**Towards a Roadmap for Future Research**  
(main area: foundations)

***Quantum Cryptography – a novel technology for secure communication***

(Submitted by ARC Seibersdorf Research GmbH / Austria)

Today's most secure cryptography techniques are threatened by entirely new approaches in computational technologies. The advent of the quantum computer will break many procedures of data encryption that seem to be unbreakable at the moment. So completely new technologies to face this problem have to be developed.

In the last decade a number of primarily academia based research groups have demonstrated that quantum physical effects can be used to simultaneously generate an absolutely random bit-sequence at two distant locations. Due to the principles of quantum physics any eavesdropping attempt of this bit-sequence cannot remain unnoticed by the legitimate parties. The bit sequence can therefore be used as a key for further encryption that cannot be broken even by quantum computers.

This method called Quantum Cryptography has reached a state of maturity that makes it possible to develop a corresponding device. Although there are still many unsolved problems to this end, which fall in the domains of quantum physics, (opto)electronics, quantum information theory, and cryptography, it is now obvious that with a reasonable degree of effort it would be possible to develop a practically usable industrial prototype within the next five years.

ARC Seibersdorf research in close co-operation to the Institute of Experimental Physics of the University of Vienna, lead by Prof. Anton Zeilinger, has started a project that aims at developing such a prototype and bringing it to market. This project will lead to the submission of a proposal for an "integrated project" within FP6 IST.

A network of excellence engaged in future research in the area of cryptography should take into account such emerging technological perspectives as well. It appears absolutely necessary for groups working on new cryptographic methods to be informed on the advances and within this new development. While the quantum cryptographic hardware necessary for the use of this technology has not very much in common with "classical" cryptography there are many points of contact with cryptography when integrating this device into existing infrastructure and networks and especially in designing protocols for secure communication, including but not limited to authentication, aspects of key distillation, choice/adaptation/implementation of encryption methods, etc..

Therefore we see a major benefit for a group dedicated to quantum cryptography to participate in STORK to get input from the experts active in this network on the one hand and to give new incentives for research and development activities to network group members on the other. Moreover we invite "classical" cryptographers to join the quantum cryptography team and to give support in the areas mentioned above.