**Prof. Dr. Johannes Buchmann**

**Director, Center for Advanced Security Research Darmstadt (CASED), Head of the Cryptography and Computeralgebra Research Group in the Computer Science Department, Technische Universität Darmstadt**

**What do you see as the greatest challenges that need to be addressed by IT security?**

In my view, these challenges are to develop security mechanisms for cyber physical systems, including smart phones, the Internet of services and social networks, and to develop appropriate cryptographic techniques that provide long-term protection and resist new threats, such as quantum computer and side channel attacks.

**Everybody is talking about cloud computing. Do you believe that cloud computing is secure?**

There are many security challenges in cloud computing. Traditional IT-security goals, such as confidentiality, must be guaranteed in the cloud. Short-term protection can be realized with available techniques, but there is no satisfactory solution for long-term protection. This becomes even more challenging when computational services in the cloud are used. The computations must be carried out in such a way that the security of the input data is preserved. This is why techniques such as homomorphic encryption are such a hot research topic.

**In 2008 you developed FutureSign, secure digital signatures. What are the key challenges to bringing these new electronic signature schemes to the market?**

We were able to present a hash-based signature scheme that requires minimum security assumptions and is also practical. In collaboration with hardware manufacturers we will demonstrate that the scheme is also useful in smart cards and other devices with limited computing resources. Standardizing the scheme will enable its use in a variety of applications.

**How will the presence of quantum computers affect cryptography?**

Quantum computers can be used to break all public-key cryptosystems that are currently used in practice. At the same time, the Internet and all other IT-infrastructures rely on public-key cryptography. For example, software updates, identity cards, and Internet browsing and shopping are protected public-key cryptography. In the presence of quantum computers, all public key schemes must be replaced. This is why the post-quantum cryptography community that develops practical and provably secure schemes that resist quantum computers is constantly growing. Although it may take many more years for large scale quantum computers to be possible, we must start now. It takes more than a decade from the invention of a new scheme to its practical application.

**What are the future trends in IT security, based on CASED research?**

We will focus on bringing security into software and hardware products by design and not only as an add-on. We have identified usability as one of the major challenges to security solutions.