

## **Approaches to Black-Box Secret Sharing from Algebraic Number Theory**

**Professor Ronald Cramer**

Professor, Mathematical Institute,  
Leiden University, The Netherlands

Head of the Cryptology and Information Security  
Research Group, CWI Amsterdam



**Date : 9 April 2009 (Thursday)**

**Time : 4.30 pm – 5.30 pm**

**Venue: SPMS-Executive Classroom 1, MAS-03-06  
School of Physical and Mathematical Sciences**

A black-box secret sharing scheme (BBSSS) for a given access structure works in exactly the same way over any finite Abelian group, as it only requires black-box access to group operations and to random group elements. In particular, there is no dependence on e.g. the structure of the group or its order. The expansion factor of a BBSSS is the length of a vector of shares (the number of group elements in it) divided by the number of players  $n$ . At CRYPTO 2002 Cramer and Fehr proposed a threshold BBSSS with an asymptotically minimal expansion factor  $\Theta(\log n)$ . This dramatically improved the previous solution by Desmedt and Frankel from the late 1980s, which had expansion  $\Theta(n)$ . At CRYPTO 2005, Cramer, Fehr and Stam further improved the results, achieving an expansion factor that is absolutely minimal up to an additive term of at most 2, which is an improvement by a constant additive factor. All these results rely on orders in number fields that admit a large enough finite subsets of elements with appropriate number theoretical properties. In this talk we survey these and some related results.

### **Speaker Biography**

Ronald Cramer (1968) is Professor at the Mathematical Institute, Leiden University (the Netherlands), where he holds the Chair in Cryptology since 2004. He is the Head and Founder (2004) of the present Cryptology Research Group at CWI Amsterdam, the national research institute for mathematics and computer science in the Netherlands. Previously (1997-2004), Cramer held research positions at ETH Zurich and at Aarhus University. He holds an MSc degree in mathematics from Leiden University (1992), and a PhD degree from the University of Amsterdam (1997).

During 2004-2007, Cramer was a Director of the International Association for Cryptologic Research (IACR). He serves on the Editorial Boards of several international journals, including Journal of Cryptology. He was Program Chair of the 27th Annual IACR EUROCRYPT and of the 11th Annual IACR PKC, and General Chair of the 4th Annual IACR TCC. Since 2004 he is junior member of the Royal Netherlands Academy of Arts and Sciences (KNAW). His research interests span most of modern cryptology, in particular theoretical cryptology and interactions with algebraic number theory, algebraic geometry, coding theory and combinatorics.

Host: Coding and Cryptography Research Group, Division of Mathematical Sciences, School of Physical and Mathematical Sciences

### **SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES**

NANYANG TECHNOLOGICAL UNIVERSITY

SPMS-MAS-03-01, 21 NANYANG LINK, SINGAPORE 637371

FAX: +65 6515 8213 TEL: +65 6513 7423