FACHBEREICH INFORMATIK
UND MATHEMATIK (ISMI)
Prof. Dr. C.P. Schnorr
Prof. Dr. T. Theobald
R. Hartung, C. Riener, A. Scemama, R. Steffens

01. Februar 2007

Vortrag in der AG "Diskrete Mathematik und Mathematische Informatik"

Am **Montag, den 26. Februar 2007, um 10 Uhr s.t.** hält

Dr. I. Shparlinski, Macquarie University, Australien

einen Vortrag zum Thema

Playing "Hide-and-Seek" in Finite Fields:
Hidden Number Problem and Its Applications.

Der Vortrag findet in Raum 612, Robert–Mayer–Str. 10, statt.
Interessenten sind herzlich eingeladen.

Abstract We describe several recent results on the hidden number problem introduced by Boneh and Venkatesan in 1996.

The method is based on a rather surprising, yet powerful, combination of two famous number theoretic techniques: bounds of exponential sums and lattice reduction algorithms. This combination has led to a number of cryptographic applications, helping to make rigorous several heuristic approaches. It provides a two edge sword which can be used both to prove certain security results and also to design rather powerful attacks.

The examples of the first group include results about the bit security of the Diffie-Hellman key exchange system, of the Shamir message passing scheme and of the XTR and LUC cryptosystems. The examples of the second group include attacks on the Digital Signature Algorithm and its modifications which are provably insecure under certain conditions.

gez. C. P. Schnorr, T. Theobald