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

Igor Shparlinski, University of New South Wales

Abstract. We describe several 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 and of the Shamir message passing scheme. The examples of the second group include attacks on the Digital Signature Algorithm and its modifications which are provably insecure under certain conditions.