Cryptography in BSS Computational Model

Ilir Çapuni[1]

Department of Mathematics and Computer Science
University of Montenegro, Cetinjski put bb
Podgorica, Serbia and Montenegro.
ilir@cg.ac.yu

Most of cryptography is based on the classical Turing model of computation. We consider the possibility of cryptographic primitives over BSS model of computation where the traditional finite field F_n is replaced with the field $\mathbf{Q}$. The very basic cryptographic primitives are the one-way functions (i.e. functions that are "easy" to compute but "hard on average" to invert). Unlike in the classical model where it is believed that one-way functions exist, in this model they do exist. It is proved that in classical BSS some basic cryptographic paradigms like encryption do not exist. We show that the situation on the "weak BSS model" differs.

In this work, we initiate theoretical investigation of cryptography on the weak BSS model over an arbitrary field (where $\mathcal{P} \neq \mathcal{NP}$), hoping that by studying cryptology in this model, a new insight for the classical model of cryptography could be obtained.

The poster will be presented during 4-9th July 2005

[1]Prof. Zarko Mijajlovic, Faculty of Mathematics, University of Belgrade, Studentski trg 16, 11000 Belgrade, Serbia and Montenegro e-mail: zarkom@eunet.yu;
Prof. Slobodan Vujosevic, Department of Mathematics, University of Montenegro, Cetinjski put bb, 81000 Podgorica, Serbia and Montenegro, e-mail: vslobo@cg.yu