ICM 1998, Berlin, Aug. 18–27

Abstracts of Short Communications and Posters

Section:

14. Mathematical Aspects of Computer Science

1991 MS Classification: not given

Khokhlov, Vladimir, Steklov Mathematical Institute, Moscow, Russia

Krawtchouk polynomials applied to analysis of an attack based on Sevast'yanov statistic

The report relates to estimates of hardness of an attack based on the Sevast'yanov statistic, which is also called the conditional prevalence. Memoryless automata containing shift registers are under investigation. Earlier estimates of the output length needed for a reliable hypotheses testing had used an approximation for the variance of the Sevast'yanov statistic. An exact formula for this variance obtained by expansion of the conditional prevalence into a series of Krawtchouk polynomials gives significantly lower bounds for the output length in real situations.