Fair e-Lotteries and e-Casinos

Eyal Kushilevitz[1]* and Tal Rabin[2]

[1] Department of Computer Science, Technion, Haifa 32000, Israel.
eyalk@cs.technion.ac.il.
[2] IBM T.J. Watson Research Center, P.O. Box 704, Yorktown Heights, New York 10598, USA.
talr@watson.ibm.com.

Abstract. In this paper we provide protocols for *fair* lottery and casino games. These fair protocols enable to remove the trust from the casino/lottery without resorting to another trusted third party, by allowing the user playing the game to participate in the generation of the specific run of the game. Furthermore, the user is able to verify the correctness of the execution of the game at the end of the run. On-line lotteries and on-line casinos have different properties and we address the needs of the two different types of games.

Keywords: e-lotteries, e-casinos, delaying functions, fair lotteries, publicly verifiable lotteries

1 Introduction

On-line gaming is a multi-billion dollar, growing industry. There are hundreds of web sites that offer various kinds of games ranging from simple lotteries to full online-casinos (where you can find most of the games that are found in real casinos like blackjack, video-poker, slot-machines etc.). The basic question that is addressed in this work is how can a user trust such a site for playing in a "fair" way. On an intuitive level, a game is fair if the chances of the user to "win" are as published by the casino owner (unfortunately, some web sites do not even bother to publish this information). In some cases, users trust the particular on-line casino based on its reputation. We note however that this should be done with caution.[1]

The first distinction that we make is between *interactive games* and *lotteries*. The typical scenario in an interactive game is a player who plays a game with the casino (a typical, popular game is blackjack). The fact that the game is interactive by its nature allows for using (interactive) protocols so as to guarantee

* Most of this research was done while the author was a visiting scientist at the IBM T.J. Watson Research Center.

[1] For example, the official web site of the New-York lottery is www.nylottery.org while if you enter www.nylottery.com you get a different web-site that until recently used to offer lotteries.

D. Naccache (Ed.): CT-RSA 2001, LNCS 2020, pp. 100–109, 2001.