Electronic Lottery Tickets as Micropayments

Ronald L. Rivest

MIT Lab for Computer Science
(RSA / Security Dynamics)
rivest@theory.lcs.mit.edu

Abstract. We present a new micropayment scheme based on the use of "electronic lottery tickets." This scheme is exceptionally efficient since the bank handles only winning tickets, instead of handling each micropayment.

1 Introduction

We present a paradigm for micropayments: probabilistic payments with "electronic lottery tickets." The probabilistic nature of lottery tickets makes payment of small values simple. For example, an electronic lottery ticket for a $10.00 prize with a 1/1000 chance of winning has an expected value of one cent. A user can pay a vendor one cent by giving the vendor such a lottery ticket.

With conventional payment schemes, a bank or broker must process each payment: the bank issues each digital coin, and processes it again when it is redeemed. *Electronic lottery tickets are the first payment scheme in which the bank does not have to process each payment*, since the bank only sees the "winners." From a bank's point of view, lottery tickets are significantly more efficient than all previously known micropayment schemes.

We assume the reader is familiar with the general notions of public-key cryptography, digital signatures, hash functions, and electronic payment schemes.

The next section introduces the details of electronic lottery tickets; following sections describe a standard implementation and variations, and discuss issues arising from this proposal.

2 Electronic lottery tickets

An *electronic lottery ticket* contains the following items of information (either explicitly or implicitly):

- The name of the *issuer* who created the electronic lottery ticket.
- The name of the *buyer* who is using the electronic lottery ticket as a means of payment. (The buyer may be the same as the issuer.)
- The name of the *recipient* who will collect the payment if the lottery ticket turns out to be a winner. We also call the recipient the "vendor," since the buyer gives the ticket to the vendor to pay for some good or service.