

ELECTRONIC TOLLING AND LOCATIONAL PRIVACY HOW TO MAKE EZ-PASS PRESERVE LOCATIONAL PRIVACY

ANDREW J. BLUMBERG AND ROBIN CHASE

OVERVIEW

In many ways, the EZ-pass system of automated toll collection devices on highways, tunnels, and bridges throughout the Northeast has been a huge success. Penetration is impressive: A majority of drivers now have the devices. But the system has the potential to substantially compromise its users' privacy.

The signal sent out by the EZ-pass transponder is unencrypted and could be read by anyone. Each transponder is uniquely linked to a particular credit card account. The states maintain databases of EZ-pass tolling data for indefinite periods of time. Uniform standards for access and use of this data do not exist. This data may be subject to demands by other private citizens, and has been successfully subpoenaed as evidence establishing the locations of alleged philanderers in divorce cases. In sum, as implemented, EZ-pass violates the locational privacy of its users.

There's no reason the system must expose its users to locational privacy violations. Over a decade ago, automated highway tolling systems which did preserve locational privacy were successfully implemented, notably David Chaum's Dynacash in Holland and Japan. Dynacash and others were based on one of the fruits of modern cryptography, *electronic cash*.

QUESTIONS AND ANSWERS ABOUT ELECTRONIC CASH FOR AUTOMATED TOLLING

Q: What's electronic cash?

A: Electronic cash functions like ordinary cash, but it is "virtual" and stored in a computer. To use it, I go to a virtual "bank" and buy some electronic cash using "real" money. Later, I spend the electronic cash on goods and services. The vendor can then redeem it for "real" money with the bank.

Q: What does "function like ordinary cash" mean?

A: When I give you a twenty dollar bill, you know you were paid. You can exchange that bill with other people. But once that bill is in circulation, no one knows who gave it to you. Once I've given it away, that bill is gone. And I can't tell just by looking at my remaining money where that particular bill went. Finally, the bank that originally provided the specific bill never knows whether I spent it or to whom I gave it.

Q: How would this work in the toll-collection context?

A: Users would purchase electronic cash and use it "charge up" their EZ-pass transponders. The transponder then pays tollbooths using the electronic cash. From the user's perspective, there would be almost no change in how EZ-pass works.

Q: But the bank knows I bought the electronic cash. Isn't my privacy violated?

A: No. Even if you buy the electronic cash from the state, the state knows only that at the beginning of the month a certain amount of money was purchased to be used for tolls – not which tollbooths were used.

Q: This seems like magic. Does this really work?

A: Yes. In fact, electronic cash systems are widely used for internet purchases. And electronic cash based tolling systems were implemented temporarily in Holland and Japan in the early 90's. Modern cryptography is amazing. But we trust it every day to secure our use of the internet (via https) and ATM machines. Modern cryptographic techniques have been proposed to help ensure the safety of electronic voting. Electronic cash is based on the same kind of technology.

Q: Could we use electronic cash to implement congestion pricing?

A: For simple congestion pricing systems, definitely! For instance, if a proposed congestion pricing plan charges a fixed amount to anyone who comes within a set boundary drawn around the downtown district during business hours, electronic cash would work well. But it doesn't work as well for more nuanced systems (e.g., the charge depends on the amount of driving within the downtown boundary), and it doesn't integrate well with privacy-preserving automated traffic enforcement solutions. For a richer approach to congestion pricing which preserves locational privacy, see our other handout.

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, STANFORD, CA 94305

E-mail address: `blumberg@math.stanford.edu`

MEADOW NETWORKS

E-mail address: `robin@meadownetworks.com`