

AN OVERVIEW OF A SYSTEM FOR IMPLEMENTING CONGESTION PRICING THAT PRESERVES LOCATIONAL PRIVACY

ANDREW J. BLUMBERG AND ROBIN CHASE

OVERVIEW

Our proposal for an implementation of a congestion pricing system that preserves locational privacy depends on following idea: Instead of having a single license plate, a driver should have many different license plates numbers — a set of “secret dynamic license plates”. Then, capturing any given license plate number doesn’t give enough information to track the driver’s movement. The hard part is then to figure out how the state can collect tolls anyway.

Here’s how the system would process the interaction of a driver (“Irving”) and the state toll collection agency (“the DMV”):

- (1) First, Irving is issued a transponder (like an EZ-pass) from the DMV. He also purchases a small “helper” device from Radio Shack. This is a little box that can plug into the transponder and also plug into a computer (and the internet) to talk to the DMV.
- (2) At the beginning of the year, Irving privately uses his helper to choose a collection of “secret dynamic license plates.” This is just a long list of very large numbers — numbers so large that there is little chance of overlap with anyone else’s numbers.
- (3) Irving’s helper digitally signs the list of license plates, and gives the signature, *but not the secret list of license plates*, to the DMV. Then the helper loads the license plates onto the transponder.
- (4) As Irving drives around, the transponder in his car rapidly cycles through the list of dynamic license plates, at the rate of a new number each second.
- (5) When Irving enters the congestion pricing zone, monitoring devices record his current dynamic license plate number as he drives past.
- (6) At the end of the billing period, Irving settles with the DMV via the following process:
 - (a) The DMV has a long list of numbers collected from drivers who have incurred tolls in the congestion pricing zone.
 - (b) Irving has a long list of secret dynamic license plate numbers, some of which were picked up by the DMV’s monitoring devices as he drove past.
 - (c) Irving’s helper and the DMV engage in a *secure two-party computation* of the charges Irving owes the DMV.

At the end of the secure two-party computation, the DMV has not learned Irving’s license plate numbers, only the amount Irving owes (see below for a discussion of how this works). Because the DMV has the signature Irving created when he chose the secret dynamic plate numbers, the DMV can be sure that Irving is paying the tolls accrued by his own secret dynamic plate numbers, even though it doesn’t know what those numbers are.

This protocol preserves Irving’s locational privacy. The information collected by the DMV does not personally identify Irving, nor does it allow them to actively track his vehicle. Nonetheless, complicated tolling information can be computed accurately during the final interaction. As a further advantage, this kind of implementation integrates well with solutions to automated traffic enforcement (e.g. stoplight cameras to catch red-light violators) that already preserve locational privacy.

SOME ANSWERS TO TECHNICAL QUESTIONS ABOUT THE IMPLEMENTATION

Q: What's a *secure two-party computation*?

A: A protocol for *secure two-party computation* is a modern cryptographic technique which solves the following kind of problem: I have a secret number, and you have a secret number. We want to compute the product of these numbers, but I don't want you to learn my secret and you don't want me to learn your secret. A *secure two-party computation* allows us to compute the product of both numbers without revealing either secret.

Q: This sounds like magic. How could it possibly work?

A: Well, it's complicated. This technology is closely related to the modern cryptographic tools that make secure internet purchases possible (e.g., https) and make ATM's safe for banking. Besides, everyone engages in a very familiar privacy-preserving computation — voting! After I vote, even though my vote can be used to decide who wins the election, no one knows how I voted. Secure two-party computations work via analogous principles.

Q: How does the state know that Irving isn't lying about the secret list of license plates he chose when this protocol started?

A: That's the point of the digital signature that Irving gave at the beginning — using it, the DMV can verify that Irving is telling the truth (via another secure two-party interaction).

Q: How does a digital signature work?

A: It produces a number associated with some piece of information (a list of license plates, for instance) that uniquely identifies that list without revealing any other information about it. Imagine that I have a "secret number", and I tell you the sum of the digits but not the number itself. It would be very hard for me to change my number without altering this sum. Digital signatures work a little like this, only much more securely.

SOME ANSWERS TO PRAGMATIC QUESTIONS ABOUT THE SYSTEM

As a general response to concerns about enforcement and potential attempts to defeat this system, it's worth pointing out that the existing situation involving physical license plates is the current gold standard for traffic enforcement. If I physically removed my license plates from my car, it might take a while for the police to catch me, because enforcement would depend solely on visual detection by a passing police officer. Because this system employs many eyes (the system's monitoring devices) in conjunction with the eyes of law enforcement, toll violators should be even easier to catch than someone driving without a physical license plate.

Q: This seems enormously complicated. Won't it be really difficult to implement?

A: It is somewhat complicated; but so was the London congestion pricing system (which is still plagued by high costs associated with collecting the tolls). But all of the hardware we require is basically bootstrapped from existing devices; most of the innovation is in the software. And the basic software for the modern cryptographic tools already exists and is in wide use.

Q: Is each person really responsible for picking a huge list of dynamic license plates and then engaging in this complicated interaction to pay tolls?

A: Well, yes, but really almost all of this is done by the helper.

Q: What about people who don't have computers?

A: Slightly fancier helpers could be designed which can connect directly to the DMV via the phone lines.

Q: What if I try to fool the system by leaving my transponder at home?

A: Just as the police stop people driving without license plates on their cars, they will be able to stop people driving through the congestion pricing zone without transponders. Furthermore, the tolling points can report that a "transponder-less" car has gone through, alerting local law enforcement.

Q: What happens if I choose not to engage in a periodic interaction to pay my tolls?

A: Drivers already engage in periodic, enforceable interactions with the state to, for example, renew their registrations. Drivers who haven't reconciled their congestion tolls could have their registrations revoked. The state might provide financial incentives to encourage early settlements of toll bills. Or the transponders could be equipped with a time-stamped authorization to operate, which expires at intervals and is renewed as part of the bill-settling process.

Q: Does this mean everyone has to have a transponder?

A: Yes; but like EZ-pass, giving them away free and having a lengthy "grace period" to let the system spread should make this requirement more acceptable to urban commuters.

Q: What about tourists and people "just passing through"?

A: No one should be "just passing through" the congestion pricing zone. By definition, these are high density urban centers. For tourists and other legitimate sporadic users, it would be easy to augment the system with prepaid transponders. Prepaid transponders might not even preserve locational privacy, although they could be designed to do so.

Q: How could the system be integrated with automatic traffic enforcement?

A: Once the "secret dynamic license plates" infrastructure is in place, it's easy to build traffic enforcement systems (or retrofit existing ones) that respect locational privacy. For instance, when a stop-light violation is detected, the vehicle's current dynamic license plate could be recorded rather than the physical license plate. Once again, via a secure two-party computation, tickets can be assessed.

Q: Do we really want freight trucks to be anonymous?

A: This system is designed primarily for passenger cars on personal business. Freight trucks engaged in commercial shipping probably should be closely monitored and tracked at all times. The point of this system is to preserve the locational privacy of private citizens using personal vehicles, while at the same time allowing the collection of congestion tolls and other traffic-management fees.

DEPARTMENT OF MATHEMATICS, STANFORD UNIVERSITY, STANFORD, CA 94305
E-mail address: blumberg@math.stanford.edu

MEADOW NETWORKS
E-mail address: robin@meadownetworks.com