

# Congestion pricing that preserves locational privacy

Andrew J. Blumberg and Robin Chase

October 18th, 2007

Our proposal for an implementation of a congestion pricing system that preserves locational privacy depends on the following idea:

Our proposal for an implementation of a congestion pricing system that preserves locational privacy depends on the 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”.

Our proposal for an implementation of a congestion pricing system that preserves locational privacy depends on the 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.

Our proposal for an implementation of a congestion pricing system that preserves locational privacy depends on the 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.

Our proposal for an implementation of a congestion pricing system that preserves locational privacy depends on the 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 interaction between a driver (“Irving”) and the state toll collection agency (“the DMV”) would work.

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).

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).

Coupons for the “helper” could be distributed, and it could be sold in many locations — the key is that Irving got it from some source that isn’t directly affiliated with the DMV.

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).

Coupons for the “helper” could be distributed, and it could be sold in many locations — the key is that Irving got it from some source that isn’t directly affiliated with the DMV.

To accomodate people who don’t have computers, somewhat fancier helpers which could be connected directly to a phone line are also possible.

Next, Irving uses his helper to pick 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.

Now, Irving needs to commit to using these license plates — otherwise he could cheat by switching them around later. But he doesn't want to reveal them to anyone.

Now, Irving needs to commit to using these license plates — otherwise he could cheat by switching them around later. But he doesn't want to reveal them to anyone.

For this, Irving uses a common and well-understood cryptographic tool, a *digital signature*. A digital signature is another number that is computed from the list of license plates. It doesn't reveal any information about the license plates, but it's hard to fake.

Now, Irving needs to commit to using these license plates — otherwise he could cheat by switching them around later. But he doesn't want to reveal them to anyone.

For this, Irving uses a common and well-understood cryptographic tool, a *digital signature*. A digital signature is another number that is computed from the list of license plates. It doesn't reveal any information about the license plates, but it's hard to fake.

Here's an illustration of how this could work: 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.

Irving uses his helper to digitally sign the list of license plates, and the helper sends the signature, *but not the secret list of license plates*, to the DMV.

Irving uses his helper to digitally sign the list of license plates, and the helper sends the signature, *but not the secret list of license plates*, to the DMV.

The important thing here is that Irving keeps his dynamic license plate numbers secret. But he discloses the digital signature, which allows the DMV to be sure he doesn't try to switch license plates later.

Irving's helper loads the license plates onto his transponder.

Irving's helper loads the license plates onto his transponder.  
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.

When Irving enters the congestion pricing zone, monitoring devices record his current dynamic license plate number as he drives past.

When Irving enters the congestion pricing zone, monitoring devices record his current dynamic license plate number as he drives past. Since the number keeps changing, the information recorded by the monitoring device can't be used to track Irving's movements.

When Irving enters the congestion pricing zone, monitoring devices record his current dynamic license plate number as he drives past. Since the number keeps changing, the information recorded by the monitoring device can't be used to track Irving's movements. This might make it seem like there's no way for the DMV to charge Irving for the tolls he's incurred — but in fact, modern cryptographic tools make this possible.

At the end of the billing period, Irving settles with the DMV via the following process:

At the end of the billing period, Irving settles with the DMV via the following process:

- 1 The DMV has a long list of numbers collected from drivers who have incurred tolls in the congestion pricing zone.

At the end of the billing period, Irving settles with the DMV via the following process:

- 1 The DMV has a long list of numbers collected from drivers who have incurred tolls in the congestion pricing zone.
- 2 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.

At the end of the billing period, Irving settles with the DMV via the following process:

- 1 The DMV has a long list of numbers collected from drivers who have incurred tolls in the congestion pricing zone.
- 2 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.
- 3 Irving's helper and the DMV engage in a *secure two-party computation* of the charges Irving owes the DMV.

A secure two-party computation is a special cryptographic tool that solves the following sort of problem:

A secure two-party computation is a special cryptographic tool that solves the following sort of problem:

I have a secret number, and you have a secret number.

A secure two-party computation is a special cryptographic tool that solves the following sort 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 is a special cryptographic tool that solves the following sort 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.

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.

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!

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.